ORDER

1600.69

FAA FACILITY SECURITY MANAGEMENT PROGRAM

March 1, 1999

DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

FOR OFFICIAL USE ONLY

PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 USC 552

Distribution: A-WXYZE-3; A-FOF-O (LTD)

Initiated By: ACO-400

RECORD OF CHANGES

DIRECTIVE NO. **1600.69**

CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL	CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL

FOREWORD

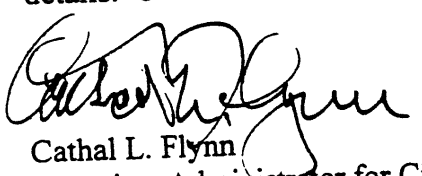
This order defines responsibilities, reiterates existing authority, and prescribes standards and procedures for the Federal Aviation Administration (FAA) Facility Security Management Program (FSMP). It establishes procedures to ensure compliance with applicable Public Laws, national security directives and policies, and Department of Transportation (DOT) orders. It also directs the Associate Administrator for Civil Aviation Security, ACS-1, to exercise, on behalf of the Administrator, overall responsibility and authority for the FAA FSMP, and to promulgate necessary operational standards and procedures to manage the program through the Office of Civil Aviation Security Operations, ACO. In order for the FAA to ensure that its facilities are ready to perform their vital functions in support of the National Airspace System, and of its regulatory responsibilities, it is the obligation of every manager and employee to ensure that they comply with their responsibilities and with security procedures and standards contained in this directive. FAA Order 1600.6, Physical Security Management Program, is undergoing revision and will exist as physical security policy only.

This order is part of a two-part general update to FAA physical security directives, comprising a streamlined agency policy directive and a separate and distinct supporting security procedures directive. Both directives will address physical security, but policy, which is only promulgated and approved by the Administrator, will be less likely to be revised with any regularity. This directive, physical security procedures directive, contains all the expanded details of the FAA FSMP and will have a tendency to change more frequently.

This order has been developed and promulgated to the affected Assistant and Associate Administrators in the affected lines of business. Each of these lines of business have participated in the FAA Order 1600.69 clearance record process as defined by FAA Order 1320.1D, FAA Directives System. Comments have been incorporated, as appropriate, to this final signed version. The following lines of business executive offices have concurred with this order: ATS-1, AVR-1, ARP-1, ARA-1, ABU-1, ARC-1, AHR-1, ADA-20, and AGC-1.

Chapter 9 and appendices 17and 18 provide for ancillary assessments in accordance with Security Risk Management methodology. These assessments will be conducted at a limited number of FAA staffed facilities to be determined by ACS-1 and the affected lines of business. The physical security assessments and inspections referred to in Chapter 2, Facility Physical Security Program, are currently the only evaluation tools used by Servicing Security Elements and apply to all FAA facilities.

This order provides the procedures directive for the FAA Facility Security Management Program and shall be used in place of FAA Order 1600.6C, Physical Security Management Program, by FAA Special Agents performing security-related functions. The update to physical security policy will be provided as FAA Order 1600.6D, but will provide only key central policy statements – not procedural details. Order 1600.6C is undergoing revision and will exist as physical security policy only.



Cathal L. Flynn
Associate Administrator for Civil Aviation Security

TABLE OF CONTENTS

TITLE

CHAPTER 1. GENERAL

100. PURPOSE. This order delineates required physical security standards and establishes objectives, procedures, and techniques for the protection of FAA employees, agency property, facilities, contractors, and the public under normal and emergency operating conditions.

101. APPLICABILITY. This order applies to all staffed FAA owned or leased facilities regardless of geographic location. FAA facilities overseas will follow the applicable United States Department of State (DOS) security directives and procedures. Physical Security assessments and inspections by FAA Regional Servicing Security Elements (SSE) of overseas locations will only be conducted as directed by the Director of Civil Aviation Security Operations (ACO-1). The DOS is responsible for providing security for U.S. Government operations overseas. **NOTE:** This does not preclude SSE's from providing security support to FAA overseas organizations after ACO-1 approval and coordination with the DOS, Bureau of Diplomatic Security. Requests for providing security support to FAA overseas organization shall be provided to ACO-1 outlining the type of security support proposed and all relevant documentation to support the request.

102. DISTRIBUTION. This order is distributed to the branch level in Washington headquarters, regions, centers, facility managers, FSMP coordinators, and limited distribution to all field facilities.

103. BACKGROUND.

a. This order establishes a FAA Facility Security Management Program (FSMP) for FAA facilities and provides for the conduct of physical security assessments and inspections to ensure program effectiveness. Facility security management, and appropriate physical security protective measures at FAA facilities are essential to reducing fraud, waste, and abuse and the risks resulting from espionage, sabotage, theft, vandalism, malicious mischief, terrorism, or other criminal acts. Any of the above actions, if not appropriately addressed, could cause injury to FAA employees, contractors, general public, damage to U.S. Government property, or complete or partial loss of FAA facilities' ability to perform critical air safety functions supporting the agency's management of the National Airspace System (NAS).

b. This order revises and updates physical security procedures for all Federal Aviation Administration (FAA) facilities and establishes standards for physical security management, control, and safeguarding of assets and facilities. This order implements Department of Transportation (DOT) Orders 4410.4, Equipment Management and Control, DOT Order 1600.23, Demonstrations in or Near Government Buildings; and DOT Order 1600.26, Department of Transportation Physical Security Program.

c. The success of facility security management requires the cooperation and support of all FAA lines of business (LOB's) in working with the appropriate FAA SSE, regional security divisions, to employ security management principles and establish physical security measures that are appropriate for each facility.

d. The Department of Justice (DOJ) in its report titled Vulnerability Assessment of Federal Facilities, dated June 28, 1995, determined that most Federal facilities do not meet minimum required standards to protect employees and assets from threats to include criminal and terrorist attack. The DOJ

report determined that physical security upgrades and continuing program emphasis on the reduction of risk to employees and assets are necessary for the majority of Federal facilities because of the environment of increased risk of such attacks. Presidential Decision Directive (PDD) 63, Critical Infrastructure Protection, dated May 22, 1998, directs every Department and agency of the Federal Government to develop and implement a plan for protecting its own critical infrastructure, directs executive departments and agencies of the Federal Government to develop plans for protecting their own critical infrastructures, and directs the FAA to implement a comprehensive program to protect the NAS from information-based and other disruptions and attacks. This order provides direction on the implementation of the required protective measures and the physical security of the agencies critical infrastructure.

104. DEFINITIONS. Appendix 1, Glossary of Terms, contains a listing and explanation of terms used in this directive. Terms will also be defined in the text when necessary.

105. AUTHORITY TO CHANGE THIS ORDER. The Director of Civil Aviation Security (CAS) Operations, ACO-1, may issue changes to this order as necessary to ensure that its provisions remain current and apply to all LOB's and organizational elements agencywide. Exceptions are changes affecting policy and delegation of responsibility, which can be made only by the Administrator.

106. OTHER STANDARDS, LAWS, DIRECTIVES AND ORDERS. Information regarding applicable Executive Orders (EO), Public Laws (PL), national security policies and procedures, and department and agency standards and directives is provided in Appendix 2, Applicable Orders, Laws, and Directives.

107. REQUESTS FOR INFORMATION. Requests for information concerning this order should be addressed to the Civil Aviation Security (CAS) Divisions (-700's) in the regions and the Mike Monroney Aeronautical Center; the CAS Staff, ACT-8, at the William J. Hughes Technical Center; and Internal Security Division, ACO-400, Office of CAS Operations, for Washington headquarters.

108. SAMPLE FORMATS, REPORTS, AND PLANS. Appendix 3, Sample Formats, Reports, and Plans, identifies and provides examples of required forms, reports, and plans that are used in support of the FSMP.

109. OBJECTIVE. The FSMP shall have the following objectives:

a. Personnel, critical assets of the agency, and facilities, shall be safeguarded from the threat of criminal, terrorist attack, and workplace violence to the levels identified in this order.

b. Management at all levels shall ensure the appropriate SSE representatives apply the FSMP and the protective measures contained in this directive.

c. FAA managers shall provide the necessary resources, including adequate funding, to protect FAA personnel and facilities.

d. Protective Measures (security management procedures, controls, and safeguards) shall be applied to the extent necessary to reduce vulnerabilities to acceptable levels as identified during physical security assessments.

e. When responsible LOB's cannot implement required protected measures to reduce an existing vulnerability(ies) due to physical, fiscal, and/or operational limitations, they may request a waiver or exception through the appropriate SSE. Waivers are only valid for a period of one year. A

new request for a waiver must be submitted if the problems continue to exist. An "exception" is a request to noncomply with a specific established requirement on a permanent basis. Requests for exceptions to policy/procedures must be submitted in writing, through the SSE to the Office of Civil Aviation Security Operations, Internal Security Division, ACO-400. The request for exception will contain the requirement, the reason for the noncompliance, and the compensatory measures being taken. See chapter 2, section 5 for further information.

f. Applies to all FAA employees and all other Federal, State, or local government workers; all contractor and subcontractor employees working for the FAA or in FAA facilities; and to military personnel assigned at FAA facilities. It includes facilities and offices of the FAA having responsibility for the control, movement, operation, commissioning, decommissioning, storage, maintenance, and/or security of agency assets. In addition to the requirements of this order, FAA operations housed within a General Services Administration (GSA) owned or leased building are also subject to applicable requirements of GSA Public Building Service Regulation P5930.17.

110. RESPONSIBILITIES OF FAA LINES OF BUSINESS (LOB's). The LOB's are the primary users of the FSMP and, as such, shall ensure that the provisions of the order are implemented.

a. Senior management within each LOB shall ensure that the contents of this order are effectively communicated to all levels of management within their organization.

b. Managers and their staffs having responsibility for conceptual development and planning for programs, projects, operations, systems, and facilities, shall implement the requirements of this order.

c. Managers and their staffs shall ensure that all LOB security education and awareness programs meet the standards set by the Internal Security Division, ACO-400.

d. Each LOB shall have an FSMP focal point(s). In some LOB's the office or service FSMP Coordinator(s) shall serve as the LOB focal point(s).

e. The Associate Administrator for Air Traffic Service (ATS) shall be responsible for:

(1) Establishing and maintaining, in coordination with ACS, ASU, and the other LOB's, a master list of FAA owned and leased facilities both staffed and unstaffed which represent the facility portion of the FAA's critical infrastructure.

(2) Determining whether ATS facilities are critical or noncritical in accordance with this order.

(3) Managing the agency funding and providing complete agency implementation of the physical security corrective actions.

f. The Associate Administrator for Research and Acquisitions (ARA) shall be responsible for:

(1) Ensuring that all submissions made through the Acquisition Management System (AMS) comply with the requirements of this order.

(2) Identifying the agency locking system and, in doing so, determine the most effective locking system for use at all FAA owned and leased facilities, in coordination with ACS-1.

111. RESPONSIBILITIES OF THE ASSOCIATE ADMINISTRATOR FOR CIVIL AVIATION SECURITY, ACS:

a. Exercising, on behalf of the Administrator, overall responsibility and authority for FAA's FSMP.

b. Ensuring that policies and procedures for the FSMP are planned, developed, and implemented agencywide.

c. Representing the program at the Joint Resources Council (JRC) on all matters concerning FAA facilities.

d. Coordinating with and supporting the LOB's and organizations as necessary to ensure that the security for all FAA facilities and associated personnel meet the physical security protective measures as stated in this order.

e. Monitoring the FSMP on behalf of the Administrator to ensure that each LOB develops and implements comprehensive security policies and procedures for its facilities and dedicates the resources necessary to support them. Deficient security controls may be reported, by the LOB, as material control weaknesses for inclusion in the fiscal year Federal Managers' Financial Integrity Act (FMFIA) report.

112. RESPONSIBILITIES OF CIVIL AVIATION SECURITY TRAINING AND DEVELOPMENT STAFF, ACS-70:

a. Is responsible for making training available to designated FAA security representatives for the facility security management program.

b. Coordinating annual requirements for facility security management training with affected LOB's.

c. Ensuring that all ACS training and awareness programs meet the standards set by the Internal Security Division, ACO-400.

d. Sponsoring and representing the facility security management training program at the national training meetings to identify resource requirements for the program.

113. RESPONSIBILITIES OF THE OFFICE OF CIVIL AVIATION SECURITY OPERATIONS, ACO:

a. Implementing the FSMP and monitor facility accreditations.

b. Ensuring the effectiveness of the FSMP through the conduct of physical security assessments, inspections, physical security program evaluations, and monitoring the status of facility physical security accreditations.

c. Coordinating with the Office of Civil Aviation Security Policy and Planning, ACP, concerning the need for and establishment of new or revised facility security policies.

d. Providing personnel required to fully support the FSMP.

114. RESPONSIBILITIES OF THE INTERNAL SECURITY DIVISION, ACO-400:

a. Ensuring that procedures are established, and adhered to, to address security vulnerabilities to the FAA and the NAS.

b. Ensuring that physical security assessments and comprehensive inspections are planned and conducted as required on FAA facilities and that required corrective actions are vigorously tracked until the discrepancy(ies) is corrected.

c. Reviewing the physical security assessments and comprehensive inspection reports that SSE's submit in the Facility Security Reporting System (FSRS) for content, accuracy, analysis, and completion of corrective actions taken.

d. Providing technical leadership, guidance, and oversight in implementing the FSMP.

e. Conducting physical security program evaluations of the SSE's as directed by ACO-1, as outlined in chapter 2, section 6.

f. Evaluating requests for and granting or denying exceptions to requirements.

g. Providing FSMP representation on departmental and interagency working groups and committees, as required or directed.

115. RESPONSIBILITIES OF THE OFFICE OF CIVIL AVIATION SECURITY POLICY AND PLANNING, ACP: Coordinating with ACO on new national policies that would affect the FSMP. In coordination with ACO and the LOB's, representing ACS in budgetary matters affecting the FSMP and undertaking, on a prototype basis facility security risk management (SRM) assessments at about 10 major FAA facilities.

116. RESPONSIBILITIES OF THE OFFICE OF CIVIL AVIATION SECURITY INTELLIGENCE, ACI: Evaluating threats to FAA facilities on an ongoing basis and providing the results to ACO and regional SSE Division Managers as appropriate.

117. RESPONSIBILITIES OF CIVIL AVIATION SECURITY DIVISIONS, -700'S (SSE's), AND THE CIVIL AVIATION SECURITY STAFF, ACT-8:

a. Implementing the provisions of this order.

b. Ensuring that staffing standards are developed to accurately reflect the number of positions required to implement the provisions of this order.

c. Identifying to ACO-400 in writing the individual(s) designated as the focal point (s) within the division or staff for FSMP.

d. Coordinating with region and center program and project managers in reviewing requirements for new construction and office space to ensure that the program or project will meet all standards established by this order. Ensure that for all facilities, a representative from the SSE will be included as an active participant on any group or team responsible for the planning and design of new facilities, or the renovation or modification of existing facilities.

e. Monitoring compliance with the FSMP through a comprehensive program of physical security assessments and inspections as required by this order.

f. Taking appropriate action to support facility managers in reducing and eliminating vulnerabilities identified during the conduct of physical security assessments and inspections.

g. Evaluating requests for and granting or denying waivers. All exceptions to requirements must be adjudicated by ACO-400.

h. Ensuring that all the data resident in FSRS is accurate and entered on a timely basis as required by the FSRS Standard Operating Procedure (SOP).

118. RESPONSIBILITIES OF ASSISTANT ADMINISTRATORS, REGIONAL ADMINISTRATORS, DIRECTOR OF THE MIKE MONRONEY AERONAUTICAL CENTER, AND DIRECTOR OF THE WILLIAM J. HUGHES TECHNICAL CENTER:

a. Ensuring that, within their respective areas of jurisdiction and control, requirements of this directive-as a minimum-are effectively and efficiently implemented.

b. Ensuring that procedures are implemented to coordinate with the appropriate security division or staff security requirements for construction of new facilities and/or modifications to existing facilities.

c. Ensuring that regions and centers incorporate the requirements of this directive into the life cycle planning and development of projects involving construction of new facilities and/or modifications to existing facilities.

119. RESPONSIBILITIES OF REGIONAL PROGRAM AND PROJECT MANAGERS:

a. Coordinating with and ensuring participation by the appropriate SSE for security support during initial phases of planning and design of new facilities and planning and design for modifications to existing facilities.

b. Including the SSE in meetings and discussions concerning the design and architectural characteristics of new facility construction or existing facility modification.

c. Ensuring that new facilities and modifications to existing facilities meet the standards and requirements of this order.

d. For larger and more critical facilities, ensuring that new facility construction and existing facility modification incorporate the requirements of this directive into the life cycle planning and development of these projects.

120. RESPONSIBILITIES OF FAA FACILITY MANAGERS:

a. Effectively implementing the FSMP as contained in this order.

b. Including the SSE in facility security planning and in implementing security policies.

c. Taking corrective actions to reduce or eliminate security vulnerabilities identified as the result of physical security assessments, inspections, or other security evaluations.

d. Establishing and implementing a Facility Security Plan (FSP) for their facility.

e. Requesting and obtaining resources as needed to implement the requirements of this order.

f. Reporting incidents and requests for visits by foreign nationals to the SSE as outlined in chapter 7 and FAA Order 1600.65, Facility Visits by Foreign Nationals and Representatives.

g. Establishing a Building Security Committee and assigning a Facility Security Coordinator as outlined in appendix 7, paragraph 14.

121. RESPONSIBILITIES OF FAA EMPLOYEES AND CONTRACTOR EMPLOYEES:

a. Complying with the requirements of this order.

b. Using good judgment and reasonable care in safeguarding and controlling government property issued officially to them or otherwise entrusted to their care.

c. Reporting to their immediate supervisors, managers, contracting officer representatives, or SSE any security weaknesses or practices involving the protection of FAA assets, including employees, facilities, and equipment.

d. Immediately reporting security incidents, outlined in chapter 7, to their immediate supervisor/ manager.

122. -199. RESERVED.

CHAPTER 2. FACILITY SECURITY MANAGEMENT PROGRAM

SECTION 1. GENERAL

200. PURPOSE. This chapter provides the guidance required for planning, coordinating, and implementing physical security assessments and inspections. Physical security assessments and inspections of FAA facilities shall be conducted in accordance with requirements specified in this order. Figure 2-1, Physical Security Overview, provides a visual summary of the complete evaluation process used for the FAA facility physical security program. Appendix 10, Physical Security Evaluation Overview, provides a complete discussion of the program. NOTE: The Security Risk Management Assessments outlined in chapter 9 and appendices 17 and 18, will be conducted by the Office of Civil Aviation Security Policy and Planning (ACP-300) and representatives from affected LOB's. Servicing Security Elements (SSE's) will conduct and participate only in assessments, inspections, and evaluations outlined in this chapter unless otherwise approved by ACO-1.

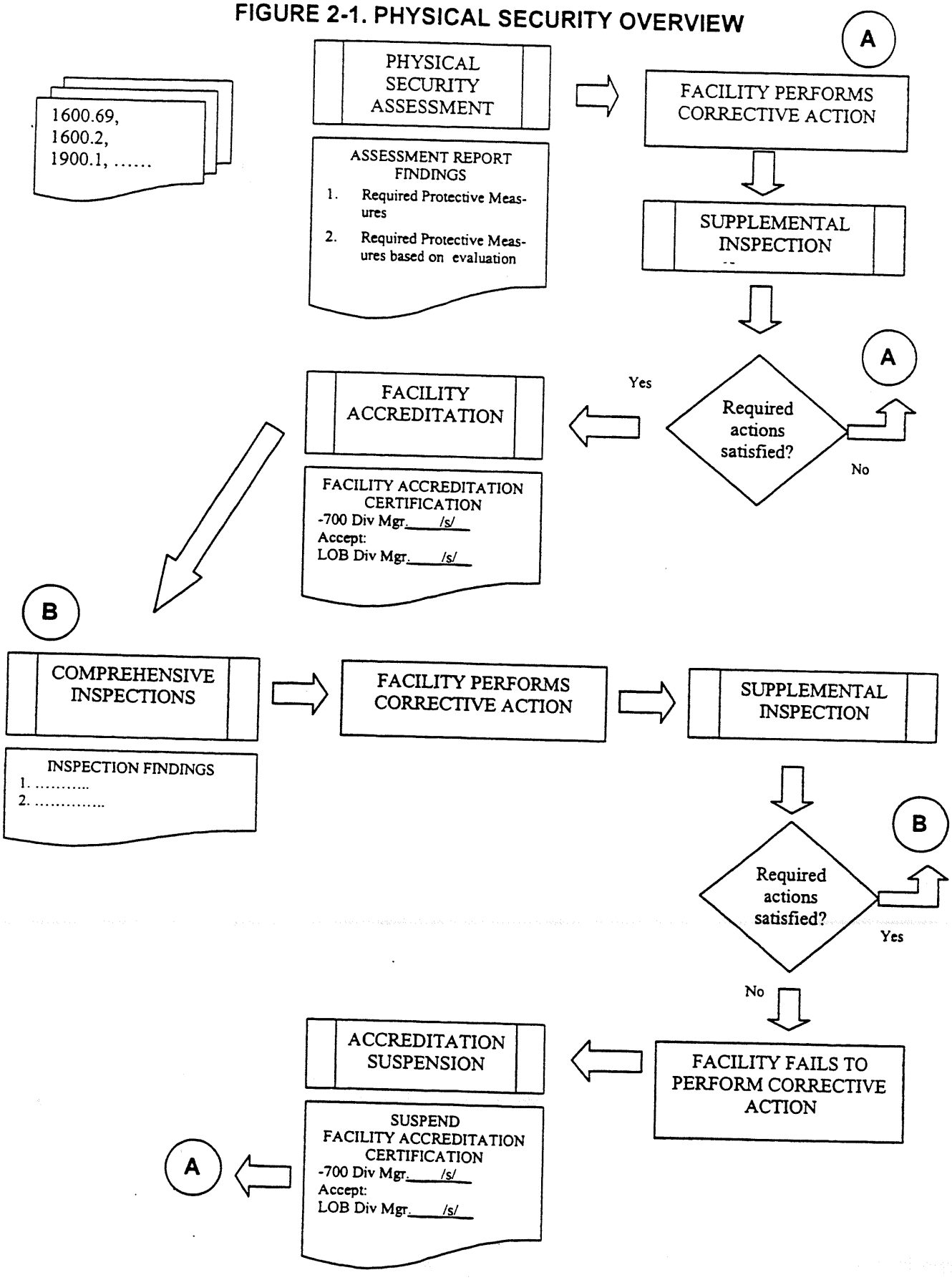
201. CRITICALITY. Criticality is the judicious evaluation of what the impact of a partial or complete loss of a facility or system would have on the mission of the agency. The criticality of a facility or asset is simply its importance to the FAA and National Airspace System (NAS). The first step in the risk analysis process is to determine, as accurately as possible, the importance or criticality of the facility, and the impact that damage or loss of the facility or disruption of the operation would have on the FAA and the NAS. In addition to the impact of loss or damage to the facility on the NAS, the criticality of the facility also depends on how readily the asset or the function it performs can be replaced.

202. ESTABLISHING PRIORITIES. FAA Facilities shall be assigned priorities based on facility criticality and criteria established in Appendix 5, FAA Facility Level Designation. Level 3 and 4 facilities shall be given scheduling priority. Once each region and center has established priorities for facilities within their jurisdiction the appropriate SSE shall take action to plan, schedule, and conduct physical security assessments and inspections as required. The SSE shall enter their assessment and inspection schedules for a fiscal year in the FSRS no later than October 30 of that fiscal year.

203. EXECUTIVE REPORTING. FSRS assessment/inspection results from regional SSE's will be reported to ACS-1 via ACO-400. ACS-1 will provide line's of business with inspection and assessment results as required.

204.-205. RESERVED.

FIGURE 2-1. PHYSICAL SECURITY OVERVIEW



SECTION 2. PHYSICAL SECURITY ASSESSMENTS AND INSPECTIONS

206. DESCRIPTION. Physical security assessments and inspections are on-site evaluations conducted by the SSE to determine if security requirements in this order are being achieved and whether they are effective against local and regional threats and vulnerabilities. The physical security assessment will augment the FSMP by identifying actual threats and vulnerabilities that must be addressed with protective measures. Physical security inspections shall provide follow up to determine whether the FSMP is being implemented properly, accreditation requirements are still being met, and generally that all security protective measures are functioning as intended.

207. PHYSICAL SECURITY ASSESSMENTS. A physical security assessment is required of all staffed facilities and is the basis for determining facility accreditation. The assessment is planned and conducted by the SSE in accordance with the frequency and procedures established in appendices 5 and 10 respectively. The time required to conduct an assessment will vary with the size and criticality of the facility and number of team members conducting the assessment. The SSE shall notify the facility manager and the appropriate LOB management of the planned assessment. Participation in the assessment will be at the discretion of the LOB management. The assessment shall consist of an on-site examination of the facility, the local threats and vulnerabilities that might exist, and determination of the overall risk level to the facility. Assessment reports shall provide a brief discussion of meaningful threats, vulnerabilities, overall risk level assigned, and will prioritize required protective measures with estimated costs for each protective measure. The SSE will provide estimated costs to aid facility managers and their management in planning for corrective actions. The written assessment report will identify:

a. Required Protective Measures. These security measures are identified in chapters 3 and 6 and must be implemented before the facility manager can request accreditation.

b. Required Protective Measures Based on Evaluation. These are security measures identified within the assessment by the SSE, when the threat, vulnerability and risk (TVR) analysis indicates that the overall risk to the facility is "high." Specific protective measures shall be developed by the SSE for the assessed facility to lower the risk level to an acceptable level. The protective measures "based on evaluation" identified in chapter 3 shall be applied for purposes of lowering risk levels from high to acceptable levels (medium or lower). The SSE when recommending other protective measures that are not specifically called for in this order shall provide written justification for their use.

208. CONDUCT OF PHYSICAL SECURITY ASSESSMENTS. Where appropriate and whenever possible, the assessment cadre shall consist of several team members selected by the SSE. Team members may be members from the: SSE staff; applicable LOB; FAA headquarters elements, or other SSE's. Physical security assessments conducted by ACO-400 as part of its overall monitoring and oversight responsibility shall include representation from responsible field SSE's. The FSRS checklist is a valuable tool that shall be used during the conduct of physical security assessments.

209. PHYSICAL SECURITY INSPECTIONS. Physical security inspections are an integrated part of the FSMP. Once a security assessment has been conducted, inspections are scheduled on a regular ongoing basis to determine whether the FSMP is being implemented properly, accreditation requirements are still being met, and generally that all security protective measures are functioning as required by this order. There are two basic types of FAA inspections: comprehensive and supplemental.

a. Comprehensive Inspections. A comprehensive inspection is an on-site review of the status of all security program areas for a facility. It is also designed to monitor overall facility compliance with required protective measures identified during previous assessments or inspections. Comprehensive inspections also serve to evaluate the significance of changes in the facility that could require additional protective measures.

b. Supplemental Inspections. Supplemental inspections are narrower in scope than comprehensive inspections. They are usually conducted as follow-ups to monitor progress on protective measure implementation from previous assessments and inspections, as a response to an incident, to evaluate a facility prior to issuance of accreditation certification, or as directed by the SSE. The previous FSRS report shall be used to conduct supplemental inspections.

210. CONDUCT OF INSPECTIONS. Inspections shall include a follow-up on the status of required protective measure implementation from previous inspections or assessments. The SSE shall report the status of all required actions identified in previous reports and indicate whether or not they have been implemented. The FSRS checklist shall be used during the conduct of inspections.

211. TRACKING REQUIREMENTS. All findings shall be individually tracked within FSRS and noted as cleared when the SSE verifies that the protective measures have been appropriately implemented. Written follow-ups shall be submitted to the appropriate manager when corrective actions for implementing required protective measures are not implemented within the timeframes noted in the assessment or inspection.

212.-219. RESERVED.

SECTION 3. FACILITY THREAT ANALYSIS

220. THREAT, VULNERABILITY, AND RISK (TVR) ANALYSIS. Included in the physical security assessment is an analysis of the threat, vulnerability, and risk to a facility. Vulnerabilities and threats to a facility are analyzed using a TVR analysis tool. The final risk level assigned will include a valid intelligence evaluation for any verified terrorist threat information. The overall results of the analysis are formulated into a risk rating for each facility. This risk rating is utilized to determine whether additional protective measures may be required for a particular facility in order to reduce the overall risk to an acceptable level and allow the facility to receive accreditation.

221. TVR METHODOLOGY. In order to identify the risk level of a particular facility, the threats and vulnerabilities are identified for use in the FSRS TVR analysis tool. Threats are identified as events such as criminal activity within the facility, criminal activity within the local area of the facility, law enforcement response times, and verified terrorist threats. Vulnerabilities are assessed in the areas of perimeter security, entry security, interior security, and security planning. All threats and vulnerabilities are assigned specific weights by the TVR tool and are averaged for an overall risk rating of Low, Medium, or High. Once all FAA required protective measures are implemented, facilities, which fall into a "High" Risk Level, must implement additional specific protective measures until the rating is reduced to an acceptable risk level. The TVR is also utilized for assessing a risk level for facilities still in the design phase to ensure the appropriate protective measures are included in the facility design stage. ACI will evaluate threats to FAA facilities on an ongoing basis and provide the results to ACO and regional SSE Division Managers as appropriate.

222.-229. RESERVED.

SECTION 4. FACILITY SECURITY REPORTING SYSTEM (FSRS)

230. PURPOSE. The procedures and responsibilities covered in this section establish the Facility Security Reporting System (FSRS) as the process and reporting format to be used by all elements of Civil Aviation Security (CAS) to report data obtained as a result of physical security inspections, assessments, and incidents at FAA facilities agencywide. The manager of each region and center CASD/staff will designate, in writing, assigned physical security specialists to be the primary and alternate program managers for FSRS within their respective area of jurisdiction to provide functional expertise as necessary. Regional technical support personnel shall be made available to assist in matters involving data or technical problems. The FSRS program manager is responsible for maintaining the integrity of the data contained in FSRS.

231. RESPONSIBILITIES. Regional and center division and staff managers are responsible for ensuring that the requirements of this order are met and that FSRS is fully implemented within their respective areas of jurisdiction. The FSRS Standard Operating Procedures (SOP) will serve as the guidance document outlining responsibilities of the regional and national FSRS program manager and users, the national FSRS technical coordinator, as well as requirements for scheduling, input, and reporting information in FSRS.

Headquarters associate administrators with access to FSRS shall restrict access to only those approved by ACO-400. Any headquarters LOB needing access to FSRS shall submit a request in writing to the Office of the Associate Administrator for Civil Aviation Security, ACS (ATTN: Manager, Internal Security Division, ACO-400).

232.-249. RESERVED.

SECTION 5. ACCREDITATION, WAIVERS, AND EXCEPTIONS

250. ACCREDITATION OBJECTIVE. Physical security accreditation is an assessment process designed to assist facility management in applying the standards of the FSMP to reduce security risk and vulnerability at their particular facility. It accomplishes this objective by conducting a physical security assessment in order to advise the facility manager of what protective measures are required, if any exist, to receive accreditation certification. The protective measures identified in the physical security assessment report are based upon the requirements of this order, other applicable orders, and directives.

251. APPLICABILITY. Accreditation is required for all staffed FAA owned or leased facilities, to include federal contract towers (FCT).

252. ASSESSMENT FOR ACCREDITATION. The physical security assessment is conducted by the SSE to evaluate compliance with the requirements of this order, other related FAA security orders, regulatory requirements, and reduction of security risks to a satisfactory level.

253. SCHEDULING OF PHYSICAL SECURITY ASSESSMENT. Physical security assessments are required for all FAA staffed facilities and shall be scheduled by the SSE, in coordination with the LOBs, with priority being given to the larger and more critical FAA facilities. An assessment may also be scheduled to meet special requirements when considered necessary by the SSE's manager. Facilities shall be evaluated for FAA Order 1600.69 accreditation certification within the normal cycle of facility assessment/inspection requirements established by FAA Order 1650.7, Office of Civil Aviation Security Operations Program Guidelines.

254. ACCREDITATION REQUIREMENTS. Facility accreditation certification is based upon the facility having implemented all protective measures required by this order, and other applicable security related orders. The accreditation process as outlined in this section shall become effective for all FAA staffed facilities on May 1, 1999.

255. PREVIOUS ACCREDITATIONS. Accreditation certifications granted prior to this order were based upon the predecessor FAA Order 1600.6C. These earlier accreditations issued under FAA Order 1600.6C will not be cancelled and are not time dependant. Accreditations granted under FAA Order 1600.6C will be upgraded to the newer FAA Order 1600.69 accreditation only after the physical security assessment has been conducted using the requirements stated in Order 1600.69, the required protective measures have been implemented and verified by the SSE, and the new 1600.69 based accreditation certification is granted. A period of up to three years after the assessment report shall be granted to facilities previously accredited under FAA Order 1600.6C to implement new required protective measures under FAA Order 1600.69.

256. DETERMINATION OF ACCREDITATION. The physical security assessment report shall identify types of findings: required protective measures and required protective measures based upon evaluation of local conditions. The facility manager, in cooperation with their regional LOB management, must resolve every required action in order to receive accreditation certification. The expectation is for the facility manager to expeditiously resolve all findings as soon as practical in order to become accredited. Upon completion of all required findings, the facility manager shall affirm in writing that the corrective actions have been accomplished and request the SSE to grant accreditation certification. The SSE will perform a supplemental inspection to affirm that the protective measures were properly implemented. FAA facilities will have up to three years to implement identified protective measures and request physical security accreditation. On-site reevaluations of implemented protective measures

must be accomplished prior to accreditation being granted. On-site evaluation of completed protective measures may be waived for administrative type matters (plans, key inventories, assignment of custodians, etc.).

257. REQUIREMENT FOR CORRECTIVE ACTION. The facility manager is required to respond as to required corrective actions for all assessment findings within 60 days. Using FSRS, SSE's will report the closure of open required actions to ACO-400.

258. FOLLOW-UP PROCEDURES. When a physical security assessment report identifies findings for required corrective action, the SSE will partner with the facility manager and applicable LOB to focus on the resolution of problems/barriers confounding accomplishment of the corrective actions. The manager of the SSE shall ensure that required corrective actions are followed up and tracked until they have been completed and the facility manager can request accreditation certification.

259. ACCREDITATION OFFICE. The SSE division manager supporting the facility will control accreditation certification. The official designated as authorized to sign the accreditation certification letter accepting accreditation from the SSE division manager will be the affected LOB division manager.

260. ACCREDITATION LETTER. The accreditation certification letter is a formal notification signed by both the SSE division manager and the affected LOB division manager to the facility manager stating that the assessed facility meets the accreditation requirements. The accreditation certification letter should be issued by the SSE division as soon as possible (inclusive of supplemental inspection whenever applicable) upon receipt of the facility manager's letter stating satisfactory completion of all required corrective actions identified in the physical security assessment report. The SSE manager will ensure follow-up procedures are conducted to verify completion. Upon verification by the SSE, the accreditation letter will be issued within 15 days.

261. DISTRIBUTION OF ACCREDITATION LETTERS. The SSE will utilize FSRS to generate the accreditation certification letter and to document the status of the facility within the FSRS database. The SSE will retain the original, update FSRS status, and provide a copy of the signed original to the appropriate division manager, facility manager, and ACO-400.

262. DURATION OF ACCREDITATION. The facility accreditation certification is not time dependant. The facility manager is required to continually meet the requirements of FAA Order 1600.69. Reference paragraph 263 for conditions or factors that may affect the overall facility and the accreditation certification.

263. CHANGES AFFECTING ACCREDITATION. Physical security assessments of a facility may be affected by a number of factors including changes in the environment, mission changes, increased threat levels, new construction, etc. The facility manager is responsible for advising the SSE of any significant changes, such as new construction, that are planned.

264. ACCREDITATION SUSPENSION. Accreditation certification may be suspended at any time by the SSE's division manager, if in the judgement of the SSE, their exists a significant condition or a violation of a previously acceptable FSMP that had been in compliance with FAA Order 1600.69. The SSE's division manager will advise the facility manager, appropriate division manager, and LOB FSMP focal point(s) in writing (and in FSRS) of the conditions and the required actions needed to rectify the problems. The facility manager must take action to rectify the required actions within 90 days or have firm plans in process to correct the problems within a reasonable period of time, as determined by the SSE. If no action, planned action or reasonable plan is proposed within 90 days, the facility accreditation certification can be suspended. The SSE shall prepare an accreditation suspension letter for signature by both the SSE Division and affected LOB Division managers. The SSE shall simultaneously alert ACO-400 and ACO-1 regarding the action taken via FSRS. Suspension of accreditation information will be entered into FSRS and may be reported in the fiscal year FMFIA report as a material internal control weakness by the affected LOB.

265. WAIVERS AND EXCEPTIONS TO REQUIREMENTS. Facility managers are required to comply with all security requirements in this order, however, there may exist mitigating operational, physical, or resource circumstances that may delay, prevent, or preclude some of these requirements from being met. Requests for waivers and exceptions must be in writing to the SSE from the facility manager(s) via the applicable LOB . The request must cite the finding of the assessment/inspection, the cited requirement, a description of the condition and a description of the alternative protective measures(s) and how it establishes an equivalent level of security. The lack of budget, resources, or staff may not, in of themselves be used for justification for issuance of a waiver. An alternative protective measure establishing a level of security equivalent to that of the required protective measure must be established. The SSE division manager can grant a waiver for a period of up to 1 year from the date of approval. The SSE division manager may extend waivers, not to exceed an additional year, after review and approval. Waiver approval correspondence shall be generated by the SSE using FSRS, and a copy of the waiver shall be sent to ACO-400. The SSE will forward exceptions to requirements to ACO-400 for resolution. The SSE will update that information into FSRS upon ACO-400 resolution.

266.-269. RESERVED.

SECTION 6. PROGRAM EVALUATIONS

270. PURPOSE. Physical security program evaluations are formal reviews by the Manager, Internal Security Division, ACO-400, of regional/center physical security and FSRS programs. Managers of Civil Aviation Security Divisions and staffs in regions and centers are SSE's responsible for program management, planning, and operations within their respective areas of jurisdiction.

271. PROGRAM EVALUATION. Areas evaluated during a physical security program review include, but are not limited to:

a. Whether the regional physical security program is in compliance with FAA Order 1600.69.

b. Whether the FSRS Intranet software reporting/database program being implemented as outlined by FAA Order 1600.69.

c. Whether the region is complying with the FSRS SOP.

d. Whether facility assessments and inspections are being scheduled and conducted as required.

e. Whether the conduct of physical security assessments and inspections are concise and accurate. This is based on a site visit to selected facilities.

f. Whether FAA facility accreditation procedures are being implemented.

g. Whether FAA incident reporting procedures are being conducted as required to include completing all information screens.

h. Whether all regional FAA staffed and unstaffed facilities have been entered into the FSRS database.

i. Whether the region/center is in compliance with any FAA Administrator directed General Notices (GENOTs').

272. OTHER AREAS. Physical security program evaluations shall also include reviews of any high interest topics identified by the DOT Office of the Inspector General, Government Accounting Office, Commissions, or as directed by ACO-1. Program evaluations will be conducted at least triannually by ACO-400 staff personnel.

273.-299. RESERVED.

CHAPTER 3. PHYSICAL SECURITY PROTECTIVE MEASURES

300. PURPOSE. This chapter sets forth standardized protective measures for FAA facilities. These protective measures, as identified within the facility's physical security assessment report, must be accomplished prior to granting facility physical security accreditation. The protective measures presented here, along with those risk reduction measures identified in assessments for new facility or modification projects, shall be incorporated into those projects beginning at budget review and conceptual phases continuing through to commissioning and capitalization phases. Protective measures are essential in establishing a baseline of protection for all FAA assets, including employees, facilities, and the operational mission. This baseline ensures that all FAA assets are provided a reasonable level of protection and employees are afforded a reasonably safe work environment. Protective measures provide a baseline of security that ensures access to FAA facilities and employees is reasonably restricted to authorized personnel. Required levels of protection not only provide protection to agency assets, but also reduce potential problems arising from inadvertent encroachment onto a facility site. The failure to apply the standards established by this order may unnecessarily put FAA employees, the operational mission, and facilities at risk. Conversely, implementation and adherence to this order will provide a reasonable degree of protection for facilities and provides a point from which to determine what, if any, additional protective measures are required. The provisions of the required protective measures presented in this chapter may not be bypassed, eliminated, reduced, or substituted without direct coordination and approval by waiver or exception. Waivers and exceptions to this order shall be in accordance with the provisions of paragraph 265. Any facility or site location not meeting the required protective measures must be considered an unsecured facility and will not receive facility security accreditation and will be reported as a major finding by ACS to the appropriate LOB.

301. OBJECTIVE. To establish physical security protective measures, standards for new and existing FAA facilities, FAA leased facilities, and FAA leased office space.

302. CONCEPT OF PROTECTION. Every FAA facility requires some degree of physical security to provide adequate physical security safeguards for FAA employees, facilities, and to safeguard U.S. Government property and assets from loss, theft, damage, unauthorized use, criminal acts, espionage, sabotage, and terrorism. The type and degree of physical security protective measures applicable to a specific facility will depend upon the assets to be protected, the criticality of the facility and its vulnerability as determined by physical security assessments. Facility managers are responsible for ensuring that adequate physical security safeguards are provided for U.S. Government property and assets under their control. The SSE is responsible for ensuring that facility managers are informed of the safeguarding requirements for their facility through the assessment and inspection process. Appendix 3, page A3-1-9, applies to all FAA leased or owned facilities.

303. BASIC DESIGN STANDARDS. Crime Prevention Through Environmental Design (CPTED) techniques shall be employed as much as possible to reduce the vulnerabilities to criminal activity. Facility design shall take the comprehensive approach and support physical security protective measure objectives of safeguarding personnel and the protection of FAA equipment and facilities. Physical security objectives shall be considered in all decisions, from selecting architectural drawings and materials, to the placement of trash receptacles, and to designing redundant critical systems. Chapter 6, New Facility Design and Appendix 9, Requirements For New Facility Construction, Renovation, and Leased Space, lists additional measures that are required for new facilities, new construction, and/or leased

space. All new design and construction projects will be reviewed and when possible will incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards during the design and planning stage. Where setback distances cannot be met, the SSE may recommend additional protective measures based on the results of the physical security assessment.

304. SETBACK DISTANCE. Where feasible for new FAA facilities, an exterior setback distance of a minimum of 300 feet and an interior set back distance of 100 feet shall be a planning goal.

305. FACILITY SECURITY GUARD CHECKPOINT. For FAA facilities employing a security guard force, a security guard house shall be provided at the site perimeter. Fenced FAA facilities employing electronic card access systems shall configure the main entrance gate with an automated entry control system (AECS) and closed circuit television (CCTV) for visual assessment capability.

306. GUARD FORCE. A well trained and equipped security guard force provides management with an effective means for implementing and monitoring the provisions of the FSMP at major and or critical FAA facilities where the physical security assessment has determined the need for a security guard force. The guard force should be used as an extension of management and, when properly supervised and employed, represents a major capability for risk reduction through effective implementation of management's FSMP policies and procedures. Where a contract guard force is required, armed security guards shall be employed.

307. DETERMINATION OF NEED. Managers of FAA facilities shall coordinate with the SSE to evaluate the need for contract security guard support for existing facilities where guards are not already required. Appendix 13, FAA Contract Guards, depicts criteria that shall be considered in the decision to employ a contract security guard force. For facilities that have contract security guard service, the facility manager shall coordinate with the SSE to ensure that the security guards are being used in the most effective manner to accomplish facility goals under the FSMP. Chapter 4 and appendix 13 establish the requirements for all providers of contract security guard services to a FAA facility. The SSE will ensure, during its physical security assessment and inspection coverage of a facility, that all FAA requirements for contract security guard service have been met. SSE's are responsible for ensuring that the information contained in appendix 13 is included in any Request for Bid or Statement of Work for contract security guard services prepared at all regions and FAA facilities. The manager of the FAA office requesting contract security guard services shall obtain concurrence from the SSE for any Request for Bid or Statement of Work for security guard services or any other security related services prior to submission of the request to the appropriate contracting office.

308. BOMB THREATS AND INCIDENTS. All FAA facilities will include specific verbiage and instructions in their individual facility security plans for bomb threats and bomb incidents. Specific requirements and guidance are provided in appendix 7, sections 3 and 4.

309. FAA FACILITY PROTECTIVE MEASURES. Tables 3-1 through 3-4 and 3-1a through 3-4a depict protective measures that shall be incorporated into FAA facilities by facility level and type. Required protective measures are baseline standards that are required by facility type and security level. Required protective measures based on evaluation are those that may be required in addition to the baseline protective measures to further reduce risk where appropriate. Appendix 11 identifies the minimum protective measures that shall be in place at existing child care centers (CCC).

310.-399. RESERVED.

TABLE 3-1. PERIMETER SECURITY PROTECTIVE MEASURES

LEGEND ● Required Protective Measure O Required Protective Measure (Based on Facility Evaluation) -- Not Applicable **Facility Security Level**	Perimeter fencing	Perimeter lighting	Standard FAA warning signs	Control of facility parking	Control of adjacent parking	Post signs and arrange for towing of unauthorized vehicles	ID system and procedures for parking (placards, decal, etc)	CCTV surveillance cameras with time lapse video recording & signage	Perimeter IDS
Security Level 4									
FAA National Headquarters	O	●	O	●	O	●	●	●	O
FAA Technical Center	●	●	O	●	O	●	●	●	O
FAA Aeronautical Center	●	●	O	●	O	●	●	●	O
Regional Office Headquarters	O	●	O	●	O	●	●	●	O
Security Level 3									
ATCSCC	●	O	●	●	O	●	●	●	O
ARTCC (NNCC where applicable)	●	O	●	●	O	●	●	●	O
ATCT (Level 5)	●	O	●	●	O	●	●	●	O
CERAP	●	O	●	●	O	●	●	●	O
Combined TRACON	●	O	●	●	O	●	●	●	O
Security Level 2									
ATCT (Level 3-4)	O	O	●	O	O	O	O	O	O
ARSR	O	O	●	O	O	O	O	O	O
ARSR/JSS	●	O	●	●	O	●	-	●	O
AFSFO / SMO	O	O	O	O	O	O	O	O	O
AFSS	O	O	●	●	O	O	O	O	O
CASFO	O	O	O	O	O	O	O	O	O
CMO	O	O	O	O	O	O	O	O	O
FSDO/ACO	O	O	O	●	O	O	O	O	O
RAPCON	O	O	●	O	O	O	O	O	O
Security Level 1									
ATCT (Level 2)	O	O	●	O	O	O	O	O	O
ADO / ATH / CASFU	O	O	O	O	O	O	O	O	O
FIO / FSM / FSS / FIFO	O	O	O	O	O	O	O	O	O
IFO / IFSS / SSC / SSU	O	O	O	O	O	O	O	O	O
MIDO	O	O	O	O	O	O	O	O	O
Security Level 1A									
ATCT (FCT) & unstaffed	O	O	●	-	-	-	-	-	-

TABLE 3-2. ENTRY SECURITY PROTECTIVE MEASURES

LEGEND ● Required Protective Measure O Required Protective Measure (Based on Facility Evaluation) -- Not Applicable **Facility Security Level**	Review receiving/ shipping procedures	Implement receiving/ shipping procedures when required	Armed Security Guards and Guard patrols	Intrusion detection system with central monitoring capability	Positive facility access control	Metal detection device at visitor entrances	Windows, Exterior Doors, walls & misc. openings	Require x-ray screening of all mail packages	Parking Lot & Entry Lighting & emergency power back-up	Peep Holes	Intercom for assessment and/or identification	Entry control with CCTV and door strikes	Agency standard Best Locks & records requirements
Security Level 4													
FAA National Headquarters	●	●	●	●	●	●	●	●	●	O	●	●	●
FAA Technical Center	●	●	●	●	●	●	●	●	●	O	●	●	●
FAA Aeronautical Center	●	●	●	●	●	●	●	●	●	O	●	●	●
Regional Office Buildings	●	●	●	●	●	●	●	●	●	O	●	●	●
Security Level 3													
ATCSCC	●	●	●	●	●	●	●	●	●	O	●	●	●
ARTCC (NNCC where applicable)	●	●	●	●	●	●	●	●	●	O	●	●	●
ATCT (Level V)	●	●	O	●	●	O	●	O	●	O	●	●	●
CERAP	●	●	●	●	●	●	●	●	●	O	●	●	●
Combined TRACON	●	●	●	●	●	●	●	●	●	O	●	●	●
Security Level 2													
ATCT (Level 3-4)	●	O	O	O	●	O	●	O	●	O	O	O	●
ARSR	●	O	O	O	●	O	●	O	●	O	O	O	●
ARSR/JSS	●	●	O	●	●	O	●	O	●	●	O	O	●
AFSS	●	O	O	O	●	O	●	O	●	O	O	O	●
CASFO	●	O	O	O	●	O	●	O	●	O	O	O	●
CMO/ACO	●	O	O	O	●	O	●	O	●	O	O	O	●
FSDO	●	O	O	O	●	O	●	O	●	O	O	O	●
RAPCON	●	O	O	O	●	O	●	O	●	O	O	O	●
Security Level 1													
ATCT (Level 2)	●	O	O	O	●	O	●	-	●	O	O	O	●
ADO / ATH / CASFU	●	O	O	O	●	O	●	-	●	O	O	O	●
FIO / FSM / FSS / FIFO	●	O	O	O	●	O	●	-	●	O	O	O	●
IFO / IFSS / SSC / SSU	●	O	O	O	●	O	●	-	●	O	O	O	●
MIDO	●	O	O	O	●	O	●	-	●	O	O	O	●
Security Level 1A													
ATCT (FCT) & unstaffed	-	-	-	O	●	-	●	-	O	-	-	-	●

TABLE 3-3. INTERIOR SECURITY PROTECTIVE MEASURES

LEGEND ● Required Protective Measure O Required Protective Measure (Based on Facility Evaluation) -- Not Applicable **Facility Security Level**	Agency photo ID for all personnel displayed at all times	Visitor controls / screening system	Visitor ID accountability system	Establish ID issuing authority	Interior Walls & Doors	Prevent unauthorized access to utility areas	Critical or restricted areas identified, posted, and access controlled	Assign and train OEP officials and conduct annual training	High risk property secured and access controlled	Provide emergency power to critical systems	FSP, OEP, and contingency procedures in place and tested	Information Security
Security Level 4												
FAA National Headquarters	●	●	●	O	●	●	●	●	●	●	●	●
FAA Technical Center	●	●	●	O	●	●	●	●	●	●	●	●
FAA Aeronautical Center	●	●	●	O	●	●	●	●	●	●	●	●
Regional Office Buildings	●	●	●	O	●	●	●	●	●	●	●	●
Security Level 3												
ATCSCC	●	●	●	O	●	●	●	●	●	●	●	●
ARTCC (NNCC where applicable)	●	●	●	O	●	●	●	●	●	●	●	●
ATCT (Level V)	●	●	O	O	●	●	●	●	●	●	●	●
CERAP	●	●	●	O	●	●	●	●	●	●	●	●
Combined TRACON	●	●	●	O	●	●	●	●	●	●	●	●
Security Level 2												
ATCT (Level 3-4)	●	●	O	O	●	O	●	●	●	●	●	●
ARSR	●	●	O	O	●	O	●	●	●	●	●	●
ARSR/JSS	●	●	O	O	●	●	●	●	●	●	●	●
AFSFO / SMO	●	●	O	O	●	O	●	●	●	●	●	●
AFSS	●	●	O	O	●	O	●	●	●	●	●	●
CASFO	●	●	O	O	●	O	●	●	●	●	●	●
CMO/ACO	●	●	O	O	●	O	●	●	●	●	●	●
FSDO	●	●	O	O	●	O	●	●	●	●	●	●
RAPCON	●	●	O	O	●	O	●	●	●	●	●	●
Security Level 1												
ATCT (Level 2)	●	●	O	O	●	O	●	●	●	●	●	●
ADO / ATH / CASFU	●	●	O	O	●	O	●	●	●	●	●	●
FIO / FSM / FSS / FIFO	●	●	O	O	●	O	●	●	●	●	●	●
IFO / IFSS / SSC / SSU	●	●	O	O	●	O	●	●	●	●	●	●
MIDO	●	●	O	O	●	O	●	●	●	●	●	●
Security Level 1A												
ATCT (FCT) & unstaffed	-	-	-	-	O	●	-	-	●	-	-	-

TABLE 3-4. SECURITY PLANNING PROTECTIVE MEASURES

LEGEND ● Required Protective Measure O Required Protective Measure (Based on Facility Evaluation) -- Not Applicable **Facility Security Level**	Contractor background check	Review and establish procedures for intelligence receipt and dissemination	Conduct annual security awareness training	Establish flexible work schedule in high threat / high risk areas to minimize employee vulnerability	Arrange for employee parking in / near building after normal work hours	Establish a Building Security Committee and Facility Security Coordinator	Establish uniform security/threat nomenclature	Establish law enforcement agency/security liaisons
Security Level 4								
FAA National Headquarters	●	●	●	O	O	●	●	●
FAA Technical Center	●	●	●	O	O	●	●	●
FAA Aeronautical Center	●	●	●	O	O	●	●	●
Regional Office Buildings	●	●	●	O	O	●	●	●
Security Level 3								
ATCSCC	●	●	●	O	O	●	●	●
ARTCC (NNCC where applicable)	●	●	●	O	O	●	●	●
ATCT (Level V)	●	●	●	O	O	●	●	●
CERAP	●	●	●	O	O	●	●	●
Combined TRACON	●	●	●	O	O	●	●	●
Security Level 2								
ATCT (Level 3-4)	●	●	●	O	O	●	●	●
ARSR	●	●	●	O	O	●	●	●
ARSR/JSS	●	●	●	O	O	●	●	●
AFSS	●	●	●	O	O	●	●	●
CASFO	●	●	●	O	O	●	●	●
CMO/ACO	●	●	●	O	O	●	●	●
FSDO	●	●	●	O	O	●	●	●
RAPCON	●	●	●	O	O	●	●	●
Security Level 1								
ATCT (Level 2)	●	●	●	O	O	●	●	●
ADO / ATH / CASFU	●	●	●	O	O	●	●	●
FIO / FSM / FSS / FIFO	●	●	●	O	O	●	●	●
IFO / IFSS / SSC / SSU	●	●	●	O	O	●	●	●
MIDO	●	●	●	O	O	●	●	●
Security Level 1A								
ATCT (FCT) & unstaffed	O	-	-	-	-	-	-	-

TABLE 3-1a. PERIMETER SECURITY PROTECTIVE MEASURES

Term	Definition
Perimeter Fencing	Standard FAA security fencing shall be constructed in accordance with Appendix 6, Perimeter and Entry Controls.
Perimeter Lighting	Where perimeter lighting is required by standard or based on a facility evaluation the requirements of appendix 6 will apply.
Standard FAA Warning Signs	Shall be posted on all standard fencing and buildings. Air traffic facilities without fencing shall have signage posted on the building in accordance with appendix 6.
Control of facility parking	Access to government parking shall be limited to government and contractor vehicles, personnel, and authorized visitors.
Control of adjacent parking	Where determined as required based on facility evaluation, parking areas adjacent to FAA facilities shall also be controlled.
Post signs and arrange for towing unauthorized vehicles	Procedures shall be established and implemented to alert employees and the public to towing policies and for the removal of unauthorized vehicles. Procedures are established in appendix 6.
ID system and procedures for authorized parking	Procedures shall be established for identifying vehicles and designated parking spaces in accordance with FAA Order 1600.25, FAA Identification Media, Official Credentials, Passports, and Vehicle Identification Media.
CCTV surveillance cameras with time lapse video recording	CCTV surveillance and recording is required where indicated. Where CCTV is required, time lapse video recording will also be employed in accordance with appendix 6.
Perimeter IDS	Perimeter IDS is required where indicated based on the facility evaluation.

TABLE 3-2a. ENTRY SECURITY PROTECTIVE MEASURES

Term	Definition
Review current receiving and shipping procedures. Modify and implement procedures where required.	Audit current standards for package entry to determine if packages are left unattended and are routinely inspected in accordance with appendix 6.
Armed Security Guards and patrols	Armed security guard contracts and guard force personnel shall be in compliance with Chapter 4, Security Response Force – Contracting for Security Officer Services, and Appendices 12, Safeguarding and Use of Firearms and Chemical Irritants, and 13, FAA Contract Guards.
Intrusion detection system with central monitoring capability	When required, all IDS and monitoring capabilities shall be in accordance with appendix 6.
Positive facility access control	Access to FAA facilities will be controlled in such a manner as to prevent unrestricted or uncontrolled entry to the facility site or interior in accordance with appendix 6.
Metal detection device at visitor entrances	Metal detectors will be used for visitors versus FAA employees.
Windows, exterior doors, and misc. openings	Windows and vents will be equipped to prevent unauthorized access in accordance with appendix 6.
X-ray screening of all mail and packages	All packages entering the building shall be subject to x-ray screening and visual inspection in accordance with appendix 6.
Parking lot and entry lighting; emergency power back-up	Parking lot and entry lighting shall be provided with emergency power back up for the protection of personnel during the hours of darkness. See appendix 6 for details.
Peep holes	Provides easy and effective visual recognition system for small offices. Inexpensive method to permit identification prior to granting access to the facility. Peep holes shall be utilized in accordance with appendix 6.
Intercom	Should also be used in combination with peep holes to permit communications with visitors before allowing access to the facility or office in accordance with appendix 6.
Entry control with CCTV and door strikes	Allows employees to view and communicate remotely with visitors before allowing access. They shall be utilized in accordance with appendix 6.
FAA standard lock system (Best), other locking devices, and records requirements.	Any exterior entrance permitting access to a FAA office or facility shall have the FAA standard lock system installed. Requirements for other types of locks and records management can be found in appendix 6.

TABLE 3-3a. INTERIOR SECURITY PROTECTIVE MEASURES

Term	Definition
Agency photo ID display	Where required, agency or contractor ID shall be displayed at all times and in accordance with Appendix 7, Interior Controls and Security Planning.
Visitor control and screening system	Visitors shall be readily apparent in all facilities. Control and screening procedures shall be in accordance with appendix 7.
Visitor identification accountability system	Facilities requiring visitor ID's shall maintain control over visitor badges and ensure their return in accordance with appendix 7.
Prevent unauthorized access to utility areas	Access shall be controlled into utility areas in accordance with appendix 7.
Critical or restricted areas identified, posted, and access controlled	Interior areas that have been designated as critical or restricted shall be identified and access controlled in accordance with appendix 7.
High risk property secured and access controlled	High risk property that is easily concealed, e.g., laptop computers, computer hardware, software, peripherals, TVs, video recorders, cameras, VCRs, shall be secured in a locked area and access restricted to designated authorized personnel only. See Appendix 8, Loss and Theft Prevention, for property requirements.
Provide emergency power to critical systems (alarm systems, radio communications, computer facilities, etc.)	Emergency power shall be provided to critical systems in accordance with appendix 7.
Examine FPSMP, OEP, and Contingency Plans. Testing is required.	Review and update FPSMP, OEP, and contingency plans and procedures for completeness. Annual testing is required in accordance with appendix 7.
Assign and train OEP officials. Conduct tests of plans.	Assignment is based on GSA requirement that largest organization in facility maintain OEP responsibility. Officials shall be assigned, trained, and a contingency plan established to provide for the possible absence of OEP officials in the event of emergency activation of the OEP in accordance with appendix 7.
Information Security	Protection of Privacy Act, FOUO, classified, and other sensitive information in accordance with applicable agency orders.

TABLE 3-4a. SECURITY PLANNING PROTECTIVE MEASURES

Term	Definition
Contractor background checks	Conduct background security checks for service contract personnel. Reference appendix 7, paragraph 15.
Review and establish procedures for intelligence receipt and dissemination	Determine what procedures exist to ensure timely delivery of critical criminal/terrorist threat intelligence data. Reference appendix 7, section 4.
Conduct annual security awareness training	Provide security awareness training for all employees. At a minimum, self-study programs utilizing videos and literature shall be implemented. These materials should provide up-to-date information covering security practices, employee security awareness, personal safety, etc. Examples of topics can be found in appendix 7.
Establish flexible work schedules in high threat/high risk area to minimize employee vulnerability to criminal activity	Where required, flexible work schedules will enhance employee safety by staggering reporting and departure times. As an example, flexible schedules might enable employees to park closer to the facility by reducing the demand for parking at peak times of the day. Parking near the building shall always remain in compliance with any GENOT in affect.
Arrange for employee parking in/near building after normal work hours	Minimize exposure to criminal activity by allowing employees to park at or inside the building.
Establish a Building Security Committee and Facility Security Coordinator (FSC)	Responsible for determining requirements for implementation of minimum protective measures requirements at it's facility. The committee shall consist of representatives from all federal agencies or co-located FAA organizations occupying the same building. Each FAA facility shall assign an FSC to act as the focal point for all security activities and requirements.
Establish uniform security/threat nomenclature	To facilitate communication, standardized terminology for alert levels should be implemented. (Security conditions have been adopted FAA wide). Reference FAA Order 1900.1F, chapter 3.
Establish law enforcement agency/security liaisons	Intelligence sharing between law enforcement agencies and FSC/BSC should be established in order to facilitate the accurate flow of timely and relevant information. Reference appendix 7, section 4.

CHAPTER 4. SECURITY RESPONSE FORCE - CONTRACTING FOR SECURITY OFFICER SERVICES

400. PURPOSE. This chapter establishes mandatory Facility Security Management Program (FSMP) standards for the contracting of private security services for FAA facilities and assets.

401. REQUIREMENT. In order to provide the trained resources to administer the FSMP, and to assure that the program remains responsive to management, a dedicated security response force organization shall be established and maintained at FAA facilities that have been determined to require facility security guards. Appendices 12 and 13 establish the required security standards for the selection and utilization of security guards at FAA facilities.

402. SIGNIFICANCE. In order to establish and staff a competent, professionally trained, and well-supervised security guard organization, it is necessary first to contract with an appropriate provider of security services. The commercial vendor who is selected to fulfill the FAA's need for a security guard organization at its major facilities is an indispensable element of an effective FSMP. For this reason, selection of a vendor for a security service contract shall be a joint effort involving facility management, the servicing security element (SSE), and the division or office having FAA contract responsibilities. The FAA facility Contracting Officer's Technical Representative (COTR) assigned for management and oversight of the security guard contract must be assigned to the facility requesting security guard service. The facility FSMP Coordinator is the logical choice for filling COTR responsibilities for the facility's security guard contract.

SECTION 1. SELECTION

403. SELECTION OF A SECURITY SERVICE PROVIDER. When preparing to advertise for the services of a commercial firm to provide security officers for FAA facilities, the following minimum criteria shall be included in all steps of the acquisition process:

a. The vendor shall be one whose primary business is the provision of contract security services.

b. The vendor shall have been in the business of providing contract security guard services for a continuous period of at least the immediate past 5 years.

c. The contractor shall provide, in writing, evidence of satisfactory provision of service to large facilities having plant and employee population characteristics similar to FAA Level 3 and 4 facilities.

d. Appendix 13, FAA Contract Guards, establishes the minimum security standards which shall be met by any provider of contract guard services to an FAA owned or leased facility.

e. SSE's are responsible for ensuring that the information contained in appendices 12 and 13 is included in any Request for Bid or Statement of Work for FAA contract guard services at all regions and centers. SSE's will evaluate during physical security assessments and inspections that these requirements have been met.

f. The manager of the FAA office requesting contract guard services shall obtain concurrence from the SSE on any Request for Bid or Statement of Work for FAA contract guard services prior to proceeding with the acquisition process. The manager will also ensure a provision is included in the Request for Bid or Statement of Work, that the U.S. Government reserves the right to award the contract to the company or entity which best demonstrates the capability to effectively fulfill the requirements of the contract and is not obligated to accept the lowest bid.

g. The FAA contract guard contractor is responsible for ensuring that all guards qualify for and continue to meet requirements for state and local licensing.

404. CONTRACTOR REQUIREMENT. The contractor shall provide supervision of their personnel to ensure compliance of all contract services. This full-time supervisory representative must be satisfactory to the COTR and the SSE.

405. CONTRACTOR RESPONSIBILITY FOR FAA CONTRACT GUARD MANUAL. Each contractor shall be required to develop and issue a current and comprehensive FAA contract guard manual (reference appendix 13, paragraph 20) to each FAA contract guard assigned to duty on an FAA facility. The manual shall be coordinated with the FAA COTR and the SSE before issuance. The manual shall contain the basic guidance issued by the contractor to all employees concerning matters of dress, maintaining good physical condition, discipline, patrolling, first aid, emergency responsibilities, apprehension of suspects and arrest powers, courtesy, communications, chain of command, and duties to be performed.

406. CONTRACTOR SUPERVISORY REPRESENTATIVE. The contractor's supervisory representative shall have had experience in facility protection at a level commensurate with the work scope of this contract. The supervisory representative shall:

a. Inspect FAA contract guards periodically during their shifts to observe their conduct from the standpoint of efficiency, conduct, and compliance with the FAA contract guard manual, FAA contract guard orders, and other applicable regulations and instructions.

b. Enter each inspection and the results thereof in the security officer daily duty log and sign the entry.

407. PERFORMANCE CRITERIA. In making the required supervisory inspection, the contractor shall determine at a minimum that the security officer is in full uniform when carrying out the duties and responsibilities of the FAA contract. The inspection shall ensure that the overall appearance and demeanor of the security officer is one that promulgates professionalism, not only during the actual inspection but also throughout the assigned shift. The contractor shall ensure that:

a. A current copy of the regulations and instructions pertaining to the contract guard post, a copy of the FAA contract guard manual, and FAA contract guard orders are immediately available at each post of duty.

b. Each contract guard has studied the orders and regulations and is thoroughly familiar with them.

c. Each FAA contract guard understands that they must comply with the orders and regulations at all times.

408. - 499. RESERVED.

CHAPTER 5. LOSS AND THEFT PREVENTION

SECTION 1. SAFEGUARDING GOVERNMENT PROPERTY

500. PROTECTION OF GOVERNMENT PROPERTY. The protection of property, including the prevention of theft, waste, and abuse of government supplies and equipment, is a mandatory responsibility for managers under the provisions of the Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255, passed in 1982. The facility manager must have an effective property management program which meets the requirements of FAA Order 4650.21, Management and Control of In-Use Personal Property, and includes the following security concerns:

a. Conduct physical inventories of accountable property as required and report promptly any unexplained shortages, known or suspected thefts to the SSE, especially for that property identified as "sensitive" or "high-risk." See appendix 8, section 1.

b. Ensure adequacy of the external and internal physical security controls.

c. All personnel responsible for protecting government property will receive security awareness training at least annually to ensure they are cognizant of their responsibilities and accountability/consequences for failure to comply in this area.

501. THEFT TARGETS. Each year as the NAS infrastructure continues to expand, FAA property record values rapidly increase. High-value items such as laptop computers, cellular phones, and electronic equipment have decreased drastically in size, lending themselves to concealment, and there are markets available for their disposal. The SSE will assist the facility manager in identifying these possible theft targets during inspections and physical security assessments and will work with the facility manager to develop appropriate protective measures to reduce identified vulnerabilities.

502. SHIPPING AND RECEIVING OPERATIONS. Regardless of the size of the FAA facility, shipping and receiving operations are extremely vulnerable to systematic theft. From a physical security perspective, the following apply:

a. Shipping and receiving area doors shall be kept closed and secure at all times when not in use. CCTV shall be used for receiving and shipping areas at large FAA facilities.

b. Deliveries, especially those containing high-value items, such as computers, shall not be left unattended. Such items shall be properly secured until processed through shipping and delivering and signed for by the intended recipient.

c. High-value items, upon receipt, shall be inventoried and a record kept of where the items were delivered and/or stored.

d. Secure holding areas with limited access shall be used to protect undelivered high-value items.

503. LOAN POOLS. Loan pools are an inviting target to theft because of the wide range of items that usually appear in the inventory (e.g., office equipment, recorders, video and motion picture equipment, and cameras). In protecting loan pools, the following requirements apply:

a. In addition to separating high risk items and securing the loan pool, administrative controls must be strictly observed. Maintaining current inventory records, establishing a limited charge-out period, and following up on overdue items, as well as limiting access to the loan pool, are all important.

b. Expendable items such as film and videotapes, which are not subject to strict accountability, shall nevertheless be protected in such a manner that they are not subject to unauthorized access and pilferage.

504. GENERAL AND SPECIALIZED STORAGE AREAS. Supplies and equipment that are stored in permanent or temporary areas or warehouses are vulnerable to theft if adequate precautionary measures are not taken. Access to storage areas containing building materials, automotive and oil supplies, tools, etc., shall be tightly controlled because of the personal use, which can be made of such items. The following requirements apply:

a. Items that are not ordinarily accounted for in the property management and control system shall be afforded protection from unauthorized access.

b. Charge-out procedures shall be established that will help to deter employees from drawing such materials for other than official purposes.

c. In large warehouses, high-risk and high-value items shall be stored separately from the general storage area in special security enclosures of wire or chain link secured by approved FAA standard combination padlocks.

505. REMOTE STORAGE AREAS. Areas that are remote from the facility pose special problems. The SSE shall work closely with the facility manager to evaluate the most effective protective measures to protect such locations. The use of IDS, CCTV, or other special security safeguards, which can be monitored from a remote location, must be considered.

506. OTHER FAA STORAGE AREAS. Navigation aids, air traffic control towers, hangars, laboratories, research and development areas, training facilities, unstaffed facilities and similar locations are vulnerable to tampering, pilferage, and interference with the operational mission. The facility manager is responsible for coordinating with the SSE to establish suitable property control and physical security safeguards for these types of areas.

507.-509. RESERVED.

SECTION 2. THEFT PREVENTION

510. THEFT PREVENTION MEASURES. An on-going loss-theft prevention program is essential at every FAA facility. Facility managers in coordination with the SSE shall develop specific plans and procedures and implement effective physical security measures to reduce and prevent the vulnerability of FAA assets to pilferage, theft or misappropriation. Developed procedures shall be incorporated into the facility security plan. The SSE will advise the facility manager on protective measures based on a physical security assessment of the risk and vulnerability associated with specific areas and operations. Protective measures considered by the SSE will include, but not be limited to, the following:

a. Establishing appropriate physical security safeguards with regard to perimeter fencing, lighting, parking area control, vehicle and pedestrian control, waterways and vertical threats, and railway control.

b. Establishing effective property removal procedures to include documentation. Interior controls identified in appendix 7 provide the framework for developing viable procedures. Facility property removal procedures shall also be included in the facility security plan.

c. Maintaining an effective key control system. Refer to appendix 6, section 6, for required procedures.

d. Management shall investigate and report all thefts and losses as soon as possible and thoroughly and provide the SSE (through their appropriate chain of command) with a written copy of their report. Major losses along with any thefts shall be reported to the SSE within 24 hours for evaluation and the possibility of further investigation.

e. At facilities with a security guard force, adequate patrols to check buildings, grounds, facility perimeters, and locations which might be used for concealing stolen property shall be implemented and included in the facility security plan. At all other facilities, management and supervisors must be aware of the potential areas in their facility that could be used for concealing stolen property.

f. Installing mechanical or electrical intrusion detection systems (IDS) where practical and where a response capability is provided to respond to an alarm condition.

g. Storing bulk quantities of high-risk items in enclosed storage areas approved for that purpose by the SSE.

h. Marking all tools and equipment by some mark or code so that U.S. Government property can be distinguished from nongovernment property.

i. Requiring charge-out procedures for all tools and high-risk equipment.

j. Ensuring that adequate inventory and control measures are established for all material, supplies, and equipment in accordance with requirements of FAA Order 4650.21, Management and Control of In-Use Personal Property.

k. All mandatory sensitive items, as defined in FAA Order 4650.21 and this order, must be controlled. Facility managers and property custodians should consider developing a hand-receipt system using FAA Form 4650-11, Memorandum Receipt, to account for the distribution of these items.

511. PROPERTY MANAGEMENT SYSTEM. There is a direct correlation between the efficiency of the property management system in effect at an FAA facility and the theft prevention program. Each is an indispensable element of the other. The Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255, requires Federal agencies to ensure that their internal accounting and administrative controls conform to the standards prescribed by the Comptroller General, and that they provide reasonable assurances that (among other requirements) funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation. The Federal Property and Administrative Services Act of 1949 and associated implementing orders from Office of the Secretary of Transportation (OST) and FAA require accountability for all government-owned property including personal property. The following considerations apply:

a. Ensure that there is a close working relationship between the SSE and the region/center property management office. The SSE will include review of property accountability and loss control procedures during the conduct of each inspection and physical security assessment.

b. The most common deficiency is failure to report (usually inadvertent) any actual or suspected thefts of "in-use personal property" that comes to the attention of the property custodian through inventory and/or other means. The FAA facility property management office will ensure that reports of suspected theft are being forwarded to the appropriate offices (i.e., SSE, region/center property management office).

c. It is not uncommon to find that lost or stolen property has been surveyed and "written off" by the property accounting office. To avoid this happening, the region/center property management office shall provide the SSE with Reports of Survey that involve high-value items or Reports of Survey that encompass several items of property possibly showing a pattern of lost and/or stolen property (monthly). As an example, committees have been formed with SSE participation to review the Reports of Survey and determine if further investigation/inquiry is needed to resolve questionable losses.

512. ACCOUNTABLE EQUIPMENT CATEGORIES. During the conduct of assessments and inspections, the SSE will include a review of the adequacy of the accountability and control procedures in effect for all accountable equipment. For a list of accountable equipment, see the current version of FAA Order 4650.21 and appendix 8 of this order.

513. REMOVAL OF PROPERTY FROM FAA FACILITIES. FAA managers are responsible for accountability and control of any U.S. Government property removed from their facility. The facility manager shall coordinate with the SSE to develop property removal and accountability procedures that will meet these objectives. Each facility manager is responsible to ensure that some type of positive control and accountability system is used. Two procedures are already in place:

a. An individual who intends to remove property from an FAA facility shall prepare a DOT F 1660.2, Property Removal Record, see Appendix 3.

b. Employees are not normally authorized to bring personal computers to the work site except under extenuating circumstances. Procedures for approval to bring privately owned computer equipment to/from the work site are found in FAA Order 1600.54, Automated Information Systems Handbook. Any employee doing so must possess the proper documentation/authorization form signifying that the employee owns the computer.

514.-599. RESERVED.

CHAPTER 6. NEW FACILITY DESIGN

600. OBJECTIVE. Every staffed FAA facility shall be accredited following the process identified in chapter 2, section 5. The optimum opportunity for requisite security features to be incorporated into any facility are during the budget-request, concept, design, construction, and capitalization phases. If incorporation of security features and protective measures is successful, the facility shall be accredited immediately prior to, or upon, commissioning. The accreditation process shall not delay commissioning of a new facility. All new construction shall establish uniform protective measures as identified in this chapter, and appendices 6, 7, and 9.

601. PROJECT MANAGEMENT RESPONSIBILITIES. Engineering LOB's for all new construction and modification projects, and the Logistics organizations, during space leasing and modifications to leases and leased space, shall provide points of contact to interface with the SSE physical security specialist and coordinate the incorporation of required protective measures into the project. The Project Coordinator/Manager shall ensure through formal correspondence that the SSE is contacted at budget submittal phase to participate in all succeeding phases of the project to include planning. The Project Coordinator/Manager shall ensure that the SSE is provided up-to-date time schedules and information, drawings, hardware schedules, specifications, and all other information and materials needed by the SSE.

602. RESPONSIBILITIES OF THE SERVICING SECURITY ELEMENT (SSE). The SSE division manager shall assign a physical security specialist as the point of contact for each facility project. The SSE shall, through assessment processes, determine protective measures required to mitigate and manage security risks, and in partnership with the cognizant LOB's, ensure those measures are incorporated into the facility at inception through to commission. The SSE shall provide the necessary funding, support, equipment, supplemental travel, and other expenses needed by the physical security specialist.

603. FACILITY MANAGEMENT REPONSIBILITIES. Managers of FAA offices or activities in the facility shall each appoint a project security representative, who shall be empowered to speak for management, and to coordinate actions with the security specialist. Common expectations include participating in the development and writing of the Facility Security Plan (FSP), identifying key control official and occupant emergency organization members, coordinating the programming, testing, troubleshooting and optimization of protective systems, training of system operators, and coordinating employee transition training, etc. The project security representative may also be called upon to participate in phased inspections, liaison between project team members, etc.

604. CONCEPT OF PROTECTION. While FAA facilities range in criticality from little impact if interrupted or loss to significant impact to the NAS and/or agency operations, including safety of air travelers, the design of facilities shall focus on deterrence rather than defense. A defended facility incorporates design characteristics which will repel attackers and/or absorb the impact of attack(s). Deterrence incorporates characteristics which emphasize control of the operational environment to the extent that the potential of a successful attack or other illegal or unauthorized act is diminished or controlled. If an attacker, criminal, or person planning unauthorized acts is confronted with an environment where the potential of discovery is high and of a successful action is low, then the probability is high that he/she will either reconsider the act or will select a different target facility. The protection of information under laws, regulations, and orders is a primary responsibility of the agency as part of the Federal Government. When sensitive information is compromised, the results may be devastating to the facility,

the FAA, national security, or the Federal Government as a whole. Loss of assets results in higher operating costs, impacts operational capability, affects staff morale, and retards overall operational efficiency. The ability to prevent, detect, respond, and recover from emergencies, such as fire, power loss, violence, etc., is critical to ensure operational capability. Deterrence, information security, loss prevention, and emergency/contingency planning and control are accomplished through the FSMP.

605. FSMP IN FACILITY PLANNING AND DESIGN. The FSMP seeks out and identifies threats and human related acts with the capability to interrupt the operational capability of the facility, cause the loss of assets, and/or result in injury or death to facility staff. The FSMP then identifies and assesses vulnerabilities that would permit the threat(s) to succeed. The FSMP then assesses the probability of the threat(s) to succeed with respect to the inherent vulnerabilities. The FSMP is used in facility planning to define the operating environment of the facility and identify threats associated with it. Security features and protective measures are then incorporated to mitigate and reduce the overall risk.

606. PROCESS.

a. New Construction. The Project Coordinator/Manager shall notify the SSE in writing of the project at the planning and/or conceptual design phase. An appointed SSE physical security specialist or team shall participate in development of the budget request and in all successive phases.

(1) Upon notification, the SSE physical security specialist shall begin collection of data and information necessary to begin a physical security assessment; i.e., facility criticality, location, etc. Additional information shall be included in the assessment as it becomes available. Including required protective measures specified in orders, regulations, security design standards, and other guiding documents, the assessment is the basis for determining security features and protective measures to be incorporated into the facility design.

(2) The design review shall be conducted from outside the perimeter, to the perimeter, to the exterior, to the interior, and from ground-level down and ground-level up. Minimum protective measures, balanced against the assessment, are incorporated into the design. Where minimum protective measures are determined to be impossible to implement or where an alternative measure must be used, a request for exception from policy shall be submitted. Security measures from the assessment shall be incorporated directly. Refer to appendix 9 for specific requirements.

(3) The physical security specialist shall attend the meetings and design reviews for new construction.

(4) The physical security specialist shall work with the Project Coordinator, project security representative(s), professionals, technicians, and specialists in the other disciplines to plan and conduct inspections of facilities under construction to validate the incorporation of security designs and assess problem areas. The SSE will also participate in the Contract Acceptance Inspection / Joint Acceptance Inspection (CAI/JAI) and commissioning process.

(5) The physical security specialist will coordinate with each project security representative to consult on the development and writing of the FSP. The FSP must be complete and signed by the management of each FAA office or activity in the facility for accreditation to be approved.

(6) Prior to occupancy, protective systems must be tested to ensure that their operation is consistent with expectations. Often times, subtle changes during design or construction phases, such as the swing of a door, may seem innocuous and undeserving of attention at the time of the change, but may have a significant impact upon the configuration and/or operation of the protective systems. Access control and intrusion detection systems must be walk-tested to ensure operational capabilities.

(7) Consideration shall be given to the feasibility of not collocating child care centers (CCC) with FAA facilities. If CCC's are included within FAA facilities, the construction requirements can be found in appendix 11.

b. Modifications To Existing Facilities.

(1) Upon notification, the SSE shall review previous surveys, inspections, assessments, current waivers, exceptions, and accreditation if applicable. The physical security specialist will coordinate with the Project Coordinator to conduct a physical security assessment to validate and update the security information and posture of the facility. Required protective measures specified in orders, regulations, security design standards, and other guiding documents, shall be incorporated and the updated assessment will be used as the basis for determining security features and protective measures to be incorporated into the facility design.

(2) The design review will include the latest assessment/inspection. It will be taken into consideration during the design review.

(3) The physical security specialist shall support the project by attendance at design reviews, supplemental inspections/assessments, and joint acceptance inspections where security protective measures are required.

(4) The physical security specialist shall work with the Project Coordinator/Manager, project security representative(s), professionals, technicians, and specialists in the other disciplines to plan and conduct inspections of facilities under construction to validate the incorporation of security designs and assess problem areas. The design specialist will also participate in the CAI/JAI and commissioning process.

(5) The physical security specialist will coordinate with each project security representative to consult on the development and writing of the FSP. The FSP must be complete and signed by the management of each FAA office or activity in the facility for accreditation to be approved.

(6) Prior to occupancy, those areas where modifications have taken place, protective systems must be tested to ensure that operation is consistent with expectations. Often times, subtle changes during design or construction phases, such as the swing of a door, may seem innocuous and undeserving of attention at the time of the change, but may have a significant impact upon the configuration and/or operation of the protective systems. Access and intrusion systems must be walk-tested.

c. Leased Space.

(1) The contracting officer shall notify the SSE in writing that a request for leased space, or a change to a currently leased space, is being reviewed and request the participation of the physical security specialist.

(2) The SSE physical security specialist shall begin collection of data and information necessary to begin security risk assessment; i.e. facility criticality, location, etc. Additional information shall be included in the assessment as it becomes available. Including required protective measures specified in orders, regulations, security design standards, and other guiding documents, the assessment is the basis for determining security features and protective measures to be incorporated into the facility design. If GSA will be the lessor, the SSE will coordinate with the Federal Protective Service (FPS).

(3) The physical security specialist shall attend the meetings and design reviews as deemed necessary. If funding is not available within the scope of the project, then the SSE shall support the specialist's attendance to the extent possible.

(4) The physical security specialist shall work with the contracting officer, project security representative(s), professionals, technicians, and specialists in the other disciplines to plan and conduct inspections of facilities under construction to validate the incorporation of security designs and assess problem areas. The design specialist will also participate in the CAI/JAI and commissioning process.

(5) The physical security specialist will coordinate with each project security representative to consult on the development and writing of the FSP. The FSP must be complete and signed by the management of each FAA office or activity in the facility for accreditation to be approved.

(6) Prior to occupancy, protective systems must be tested to ensure that operation is consistent with expectations. Often times, subtle changes during design or construction phases, such as the swing of a door, may seem innocuous and undeserving of attention at the time of the change, but may have a significant impact upon the configuration and/or operation of the protective systems. Access and intrusion systems must be walk-tested.

607.-699. RESERVED.

TABLE 6-1. NEW CONSTRUCTION SECURITY PROTECTIVE MEASURES

LEGEND ● Required Protective Measure O Required Protective Measure (Based on Facility Evaluation) -- Not Applicable **Facility Security Level**	Install protective film/ polycarbonate windows on all exterior windows (shatter protection)	Review current projects for blast standards	Review / establish uniform standards for construction	Review / establish new design standards for blast resistance	Establish street setback for new construction	Avoid leases/new facility construction where parking cannot be controlled	Leases/new facility construction should provide security control for adjacent parking	Evaluate whether to locate day care center in building with high threat activities	Compare feasibility of locating day care in facilities outside this location	Collocate agencies with similar security needs	Do not collocate high/low risk agencies
Security Level 4											
FAA National Headquarters	●	●	●	●	●	●	O	●	●	O	O
FAA Technical Center	●	●	●	●	●	●	O	●	●	O	O
FAA Aeronautical Center	●	●	●	●	●	●	O	●	●	O	O
Regional Office Buildings	●	●	●	●	●	●	O	●	●	O	O
Security Level 3											
ATCSCC	O	●	●	●	●	●	O	●	●	O	O
ARTCC	O	●	●	●	●	●	O	●	●	O	O
ATCT (Level 5)	O	●	●	●	●	●	O	●	●	O	O
CERAP	O	●	●	●	●	●	O	●	●	O	O
Combined TRACON	O	●	●	●	●	●	O	●	●	O	O
Security Level 2											
ATCT (Level 3-4)	O	●	●	O	O	O	-	●	●	O	O
ARSR/JSS	O	●	●	●	●	●	O	●	●	O	O
ARSR	O	●	●	O	O	O	-	●	●	O	O
AFSFO / SMO	O	●	●	O	O	O	-	●	●	O	O
AFSS	O	●	●	O	O	O	-	●	●	O	O
CASFO	O	●	●	O	O	O	-	●	●	O	O
CMO/ACO	O	●	●	O	O	O	-	●	●	O	O
FSDO	O	●	●	O	O	O	-	●	●	O	O
RAPCON	O	●	●	O	O	O	-	●	●	O	O
Security Level 1											
ATCT (Level 2)	O	●	●	O	O	O	-	-	-	O	O
ADO / ATH / CASFU	O	●	●	O	O	O	-	-	-	O	O
FIO / FSM / FSS / FIFO	O	●	●	O	O	O	-	-	-	O	O
IFO / IFSS / SSC / SSU	O	●	●	O	O	O	-	-	-	O	O
MIDO	O	●	●	O	O	O	-	-	-	O	O
Security Level 1A											
ATCT (FCT) & unstaffed	-	-	-	-	-	-	-	-	-	-	-

TABLE 6-1a. NEW FACILITY/RENOVATION PROTECTIVE MEASURES

Term	Definition
Install shatter proof film on all exterior windows	Where required, the application of shatter resistant material to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion. Shatter protection shall be installed in accordance with appendix 6.
Review current projects for blast standards.	Design and construction projects shall be reviewed to incorporate current technology and blast standards in accordance with Appendix 19, The FAA Blast Standard and Design Guideline.
Review/establish uniform standards for construction.	Review, establish, and implement uniform construction standards as it relates to security considerations for new construction in accordance with appendices 6 and 7.
Review/establish new design standard for blast resistance	An attempt shall be made to locate new site selections, in or within, facilities that do meet standards in accordance with appendix 9. New construction of government controlled facilities should review, establish, and implement new design standards for blast resistance.
Establish street setback for new construction.	Whenever possible, a minimum street setback shall be established for new construction in accordance with appendix 9. Every foot between a potential bomb and a building will dramatically reduce damage and increase the survival rate.
Avoid leases where parking cannot be controlled	Where possible, avoid leasing facilities where parking cannot be controlled in accordance with appendix 9. If necessary, relocate office to facilities that do provide added security through regulated parking.
Lease should provide control for adjacent parking	Where possible, avoid leasing facilities where adjacent parking cannot be controlled in accordance with appendix 9.
Assess feasibility of locating child care centers outside federal facility	If a facility is being considered for a day care center, an evaluation should be made based on the risk factors associated with tenants and the location of the facility. Compare feasibility of locating day care in facilities outside this location. Child care centers located at FAA facilities shall be in accordance with Appendix 11, Child Care Center Security Design Standards.
Collocate agencies with similar security needs.	Where possible, locate agencies with like security requirements in the same facility in accordance with appendix 9.
Do not collocate high/low risk agencies	FAA facilities shall not be collocated with high-risk agencies. Low risk agencies should not take on additional risk by being located with high-risk agencies. For details, see appendix 9.

CHAPTER 7. INCIDENT REPORTING

700. PURPOSE. Incident reporting is required in order to identify and assess the loss and damage to FAA property and facilities. It provides essential data that describes the type of incidents associated with a facility and is a key element in the development of the FAA Facility Security Management Program.

701. OBJECTIVE. The objective of the incident reporting process is to provide a timely and accurate flow of data concerning the nature and frequency of adverse events which occur at FAA facilities.

702. REPORTABLE INCIDENTS. Below is a list of examples of reportable incidents. This list is not all-encompassing and is intended to be used as a guide.

TABLE 7-1. EXAMPLES OF REPORTABLE INCIDENTS

Arson	Kidnapping	Stalking
Assault	Larceny	Theft
Bomb Threats	Loss of U.S. Government Property	Terrorism
Burglary	Misuse of U.S. Government Property	Vandalism
Carjacking	Murder	Violence in the Workplace
Civil Disturbance	Rape	Weapons Incidents
Drive-by Shootings	Robbery	
Drug Use	Sabotage	

703. REPORTING PROCEDURES.

a. All facility managers must place special emphasis on the collection and timely reporting of data concerning incidents at FAA facilities. Immediately upon knowledge of a reportable incident, all facilities are required to notify their SSE. When the reportable incident involves direct damage or vandalism to an FAA facility or involves an FAA employee, notification must be made to the SSE within 24 hours. Follow-up action includes the completion of the data collection form (Incidents against FAA Property and Facilities) and may be found in appendix 3. This form may be locally reproduced and shall be distributed to all headquarters, regional, and field offices.

b. The reporting requirements of paragraph 703a **shall not** circumvent the reporting of significant activities, incidents or events as directed within FAA Order 1990.1, FAA National Command and Control System. FAA Order 1990.1, paragraph 2-14r states, "Any FAA element that has first knowledge or receives the first report of an accident or other reportable incident is required to communicate the incident immediately through their established channels of communications through the appropriate

operations center. This procedure provides for simultaneous notification to lines of business organization and the appropriate operations center."

704. NOTIFICATION OF SSE. Upon notification, the SSE shall enter all required information into the Facility Security Reporting System (FSRS) for immediate transmission to ACO-400 (ACOFIRS). Reports of Incidents shall be complete and periodic updates are required until such time as the incident is closed and/or resolved.

705. SERIOUS OR CONTINUING INCIDENTS. Facilities which experience two or more serious or recurring incidents in a quarter **will** forward a request, in writing, for a physical security assessment of the facility. The request will be sent to the SSE through the appropriate division manager.

706.-799. RESERVED.

CHAPTER 8. FACILITY SECURITY AWARENESS

800. GENERAL. Any security program or system designed to deal with vulnerabilities and risk will prove ineffective unless an effective security awareness program supports it. The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the person understands his or her responsibilities and is capable of fulfilling them. Facility managers and security personnel cannot effectively accomplish any asset protection program without the active interest and support of every FAA employee and supporting contractor. Therefore, an important part of the FAA security program is in the initial training and recurring training of employees on security responsibilities. Security Awareness Training can be provided through formal training sessions, read and initial briefings, videos, local public safety agencies, or by the SSE during scheduled site visits. As the responsible manager for facility security awareness training, facility managers shall coordinate with the SSE in establishing viable facility security awareness programs at all FAA facilities.

801. GENERAL SECURITY EDUCATION PROGRAM NEED. A security education program must encompass all aspects of security. This includes physical security, personnel security, automated information system security, information security, and procedures for visits by foreign nationals. It must be designed to protect all assets: people, facilities, equipment, operating systems, information, and mission capabilities. Education programs of themselves do not "protect" assets...people do. The program must provide all pertinent information to make employee(s) aware of their responsibilities.

802. GOAL OF FACILITY SECURITY AWARENESS PROGRAM. The goal of the facility security awareness program is to acquaint all FAA personnel with security requirements and their required participation. FAA managers must instill compliance with security orders, directives, and procedures. A viable program will enhance the reduction of security violations by ensuring that personnel are aware of their security responsibilities, the need to follow established procedures, promptly reporting security violations to supervisors and managers, and the consequences of failing to report known violations in accordance with established procedures.

803. EMPLOYEE INVOLVEMENT. Cooperative and informed employees will report unlocked doors, suspicious visitors, thefts, and many other security incidents that may not normally be reported by an indifferent or uninformed staff. A facility manager that enlists the aid of assigned personnel and creates an atmosphere of intelligent awareness of potential dangers has taken a major step towards asset protection and loss control, as well as providing a safe and secure workplace for employees.

804. TYPES OF TRAINING. The types of facility security awareness training required are designated as orientation, refresher, and specific event notification.

a. Orientation (initial) training. This training shall be given to new employees and supporting contractors within 30 days of arrival at any FAA facility or work site. The training shall include individual security responsibilities, bomb threat procedures, information on security points of contact, reporting security incidents, protecting sensitive information, access control measures, visitor controls, and the facility security plan to include occupant emergency plans.

b. Refresher (recurring) training. Training is given on an annual basis and covers the overview of the issues provided for orientation training and new information specific to the facility. Other security issues of concern to employees must also be addressed during this training session.

c. Specific event notification. Special security measures to be used during the duration of an event will be briefed to facility employees. Specific events include VIP visits, implementation of FAA security conditions (SECONS) and readiness alert levels, local security incidents, emergency situations, visits by foreign nationals, and any other events determined by the facility manager.

805. CLASSIFIED INFORMATION. In addition to the above requirements, all persons cleared for access to classified information or assigned to positions of public trust shall receive a security briefing that details the specific security requirements of their job. This briefing shall consist of the following elements:

a. The need for protecting classified information and the adverse affects of national security that could result from unauthorized disclosure of classified information.

b. The prohibition against disclosing the above listed information to unauthorized persons or discussing or handling such information in such a way that would make it accessible to unauthorized persons. The proper physical safeguarding of classified information.

c. Requirements for the receipt, handling, storage, and transmission of classified information.

806. TRAINING DOCUMENTATION. Training records shall be kept for all types of facility security awareness training conducted. These records will include date and time and type of training (initial, refresher, special event), list of topics covered, and training location. The SSE will evaluate facility security awareness training while conducting physical security assessments and inspections.

807. TRAINING MEDIA. Various types of training media can be used to conduct facility security awareness. These include visual aids, movies, lecture handouts, security pamphlets, or any other materials approved by the facility manager in coordination with the SSE.

808.-899. RESERVED.

CHAPTER 9. SECURITY RISK MANAGEMENT (SRM) PROGRAM

900. GENERAL. The FAA has developed a comprehensive program of Security Risk Management (SRM) assessments that can be used at FAA Security Level 3 and 4 facilities. ACS-1 has determined that the SRM program will be considered an experimental facility security assessment methodology. It has been developed by ACP-300 and will be applied as a pilot program on as many as 10 level 3 and 4 facilities After this period of testing, the SRM program will be evaluated by ACS-1 for possible broader application. Until then, however, the SRM program is not a requirement and is presented within this order for information purposes along with Appendices 17 and 18.

901. PURPOSE. The SRM program is an available process for determining appropriate safeguards for FAA employees and all elements of the FAA's critical infrastructure. SRM is a logical process consisting of a series of steps that are described in detail in appendix 18. In assessing FAA facilities, security specialists and managers responsible for the facilities may use this process to identify critical assets; quantify the risks to those assets; and, where necessary, either reduce or eliminate vulnerabilities to achieve a reasonable level of risk. The Associate Administrator for Civil Aviation Security is the Executive Agent for this program.

902. OBJECTIVES OF THE SRM PROGRAM. The objectives of the SRM program include the following:

a. Protection of FAA employees, contractor personnel, vendors, and visitors to FAA facilities;

b. Protection of FAA's critical infrastructure, including those assets that are essential for the safe operation of the National Airspace System (NAS) and associated safety-related functions; (this objective supports the requirements of Presidential Decision Directive (PDD) 63, on critical infrastructure protection, and PDD 62, on unconventional threats, to include weapons of mass destruction.); and

c. Protection of government property; i.e., the assets that FAA owns, leases, or otherwise controls, as required of all federal agencies.

903. SRM PROCESS OVERVIEW.

a. In conjunction with the Servicing Security Element (SSE), the LOB's may use SRM as a logical process to determine what risks to FAA facilities are acceptable, and the type and extent of countermeasures required. The SSE, each LOB, and other major organizational elements may determine the required levels of protection through implementation of the SRM program. The LOB's determine the criticality of each asset. The combination of the threat, to the criticality and the vulnerabilities of the assets, determines the risk.

b. An important consideration is the pure risk to a facility and its assets. In evaluating pure risk, unlike business or speculative risk, the SSE and LOB assume that a criminal or violent act in or against a facility will be successful in causing damage to or loss of the facility or an asset. Therefore, they must address some pure risks immediately because of their severity and the potential for catastrophic impact on the facility. The pure risks in every FAA facility can also be identified when a facility is entering the planning and design phase.

c. All of the SRM steps are qualified and then quantified in dollars, enabling the determination as to the most cost-effective countermeasure for a specific vulnerability to be based on a cost benefit analysis. It is also through the cost benefit analysis that the FAA concentrates its resources on protecting its most critical assets and on the risks that pose the greatest danger.

904. SRM PLANNING.

a. Security risk management (SRM) plan. The SRM plan is a written document that management may use to document SRM strategies and methodologies and to identify and implement risk reduction countermeasures throughout the life cycle of an asset. It contains quantified information developed through SRM assessments, surveys, and inspections that management requires concerning asset identification, criticality, and threat. It also provides management with a means for determining what constitutes an acceptable level of risk for the assets addressed in the plan.

b. SRM planning for existing facilities. SRM planning and assessment for existing facilities, to include facilities that are to undergo major reconfiguration, are as important as for new facilities. The security risk reduction costs that may be incurred through changes in the configuration of the facility (or internal movement of functions) can increase sharply if the security vulnerability and risk factors are not identified and carefully weighed beforehand. The SRM process should begin once a decision is made to select, construct, reconfigure, or relocate a facility. SRM considerations should be developed based on an SRM assessment conducted jointly by representatives of the SSE and the LOB or, in the case of smaller facilities, by security specialists.

c. New facility design. The failure to introduce SRM factors in the initial facility planning and design phases can often prove to be a costly mistake. The architect, design engineer, and other key program personnel should be made aware of the security risks being addressed, and the risk reduction measures that are necessary to assure an acceptable level of risk. This means that SRM begins when the program or project begins and remains a continuous part of the program or project throughout its life cycle. Changes made after the preliminary site review will be expensive. While an accountable level of vulnerability and risk reduction protection at a facility is the desirable objective, it is not always attainable due to funding and other resource limitations. The following are additional SRM planning requirements for new facilities:

(1) The conceptual design, planning, and construction of FAA facilities should incorporate life cycle SRM planning as an integral part of the program.

(2) Initial feasibility analyses and conceptual designs should be assessed in terms of the security risk and vulnerability associated with the proposed assets.

(3) The Program Implementation Plan (PIP) for a facility should incorporate an SRM plan together with a projection of SRM funding required to provide acceptable levels of risk for the design. This plan should include all steps of the SRM process for which data are available and quantifiable. Where data is not available in a specific area the plan will indicate at what stage of the life cycle the data can be aggregated.

(4) Facility design concepts should be assessed initially, during the conceptual design and development stage, and as often as necessary throughout the developmental process to ensure that SRM principles and concepts are being followed and that the SRM plan is appropriately updated.

(5) The project manager and the program manager, should ensure that SRM planning methodology is made a discrete, integral, and identifiable part of the life cycle planning process in the development of a new facility. This is a logical and cost-effective method for determining the level of safeguarding required to provide an acceptable level of risk for the employees and other critical assets involved.

(6) The SRM plan for a new facility should consider all of the elements of risk and threat that pertain to the assets being protected and should identify specifically the countermeasures that are included and the cost of such measures.

(7) The plan should include provisions to ensure that the facility will meet minimum blast standards for FAA facilities that are contained in Appendix 19, The FAA Blast Standard and Design Guideline.

905. SRM ASSESSMENT.

a. An SRM assessment is a comprehensive evaluation and quantification of the vulnerabilities and risks associated with an asset or group of assets. In planning and conducting an assessment, the SSE and the responsible LOB have to coordinate closely in a joint effort, using a team of subject matter experts in the areas to be assessed. Priorities for the conduct of SRM assessments should be based primarily on the criticality determination by the LOB. SRM assessments require a team of approximately three persons augmented as needed by supporting expertise in highly specialized areas such as blast and weapons of mass destruction (WMD). Completion of an SRM assessment for a major facility will require approximately 5 working days. A survey shall be conducted to provide risk evaluation for facilities where a complete SRM assessment would not be appropriate. Inspections shall be conducted in accordance with guidance provided in chapter 6 to determine and quantify the extent to which the LOB has implemented risk reduction strategies required by an SRM assessment or survey. ACP-300 will perform assessments as directed by ACS-1.

b. Appendix 18, Security Risk Management (SRM) Assessment Procedures for Levels 3 and 4 Facilities, specifies the steps in the SRM assessment process for Level 3 and 4 facilities. Appendix 17, Security Risk Management (SRM) Assessment Procedures for Level 3 and 4 Facilities, states what an assessment team should do in preparing for and conducting an SRM assessment.

906. SUMMARY. The ultimate goal of the SRM program is to ensure that FAA facilities, personnel, critical assets, and systems are maintained throughout their life cycle at an acceptable level of risk from criminal and violent activity.

907.-999. RESERVED.

APPENDIX 1. GLOSSARY OF TERMS

1. **ACCESS CONTROL**. A method of providing security by restricting the movement of persons into or within a protected area.

2. **ACCREDITATION -- PHYSICAL SECURITY**. The process whereby the servicing security element (SSE) makes a determination as to whether or not an FAA facility meets the security standards established by this order.

3. **APPROVED BUILT-IN COMBINATION LOCK**. A combination lock, equipped with a top reading dial, that conforms to Underwriters Laboratories, Inc., Standard Number UL 768, Group IR.

4. **APPROVED KEY-OPERATED PADLOCK**. A padlock which meets the requirements of MIL-SPEC-P43607 (shrouded shackle), National Stock Number 5340-00-799-8248, or MIL-SPEC-P-43951 (regular shackle), National Stock Number 5340-00-799-8016.

5. **APPROVED SECURITY CONTAINER**. A security file container originally procured from a Federal Supply Schedule supplier that conforms to federal specifications and bears a "Test Certification Label" on the locking drawer attesting to the security capabilities of the container and lock.

6. **BREACH**. The failure of security controls that results or could result in the penetration of a facility or system.

7. **BOMB**. An explosive device capable of producing damage to material and injury or death to personnel when detonated or ignited.

8. **BUILDING SECURITY COMMITTEE**. A committee consisting of representatives from different organizations occupying a facility. The committee evaluates and applies the protective measures developed for the facility.

9. **CASUAL PILFERER**. One who steals primarily because he or she is unable to resist the temptation of an unexpected opportunity and has little fear of detection.

10. **CCTV**. Closed Circuit Television.

11. **CLASSIFIED INFORMATION**. Official information regarding national security designated Confidential, Secret, or Top Secret, in accordance with Executive Order 12958, Classified National Security Information.

12. **CLOSED AREA**. A protected area established to safeguard classified information.

13. **COMPROMISE**. The exposure of information or activities to persons not authorized access.

14. **COTR**. Contracting Officers Technical Representative

15. **CONTINGENCY PLAN**. A systematic, written plan assigning responsibilities and describing actions to be taken to reduce the impact of losses and events with the potential for large loss.

16. CONTROLLED AREA. A general term, which for the purposes of this order, consists of both "Closed Areas" and "Restricted areas."

17. CONTRACTING OFFICER (CO). A government official who, under departmental or agency procedures, has authority to enter into and administer contracts and make determinations and findings with respect to them. The designation also applies to a person who has any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

18. CONTRACTING OFFICER'S TECHNICAL REPRESENTATIVE (COTR). A government official who is located at the facility where contract services are utilized. The COTR is responsible for the day-to-day operations of the contract and ensures that the contract remains in compliance.

19. CRIME PREVENTION. The anticipation, recognition, and appraisal of a crime risk and initiation of some action to remove or reduce it.

20. CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN. A conceptual technique which uses natural and environmental factors to minimize crime.

21. CRITICAL AREA. That portion of a facility which is essential to continuity of operations, the partial or complete loss of which would have an immediate and/or serious effect on the capability of the facility to provide service or support to the National Airspace (NAS) operations.

22. CUSTODIAN. An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

23. ESPIONAGE. Overt, covert, or clandestine activity designed to obtain information relating to national security with the intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation.

24. EXCEPTION – PHYSICAL SECURITY. Relief from compliance with a specific physical security requirement.

25. FACILITY – FAA. Any staffed or unstaffed building, structure, warehouse, appendage, storage area, utilities, and components, which, when related by function and location form an operating entity owned, operated, or controlled by the FAA.

26. FACILITY SECURITY COORDINATOR. An individual security point of contact for staffed FAA facilities that would be the facility manager's representative in coordinating with the responsible SSE on security matters, to include assessments, inspections, and accreditations.

27. FACILITY SECURITY MANAGEMENT PROGRAM. The FAA's physical security program as outlined in FAA Order 1600.69.

28. FACILITY SECURITY PLAN (FSP). A systematic, written plan intended to provide a concise analysis of a facility security program; a plan that a facility manager can employ as an aid to effectively and efficiently using security resources.

29. **FACILITY SECURITY REPORTING SYSTEM (FSRS).** A system which permits the aggregation of data relevant to facility security, vulnerability, and risk and disposition of that data in an automated retrieval system.

30. **FOR OFFICIAL USE ONLY (FOUO).** A term used to designate unclassified information which is to be protected against uncontrolled release, and information which may be withheld from public disclosure under criteria stated in the Freedom of Information Act, Title 5, U.S.C., Section 552a(b).

31. **IDENTIFICATION MEDIA.** Badges, credentials, or other media used to establish the identities of FAA employees, government officials, contractors, vendors, or other individuals.

32. **INTRUSION DETECTION SYSTEM (IDS).** A combination of components, electronic, and other types that signal unauthorized attempts to enter or tamper with a protected area or object.

33. **JSS.** Joint Surveillance Site (FAA and U.S. Air Force).

34. **KEY AND LOCK CONTROL.** A formal method for identifying the location of and accounting for the keys and locks in a facility.

35. **LOAN POOL.** An area within an FAA facility where a high concentration of high risk items such as cameras, projectors, calculators, VCR's, etc., are available for assigned personnel to check out and use at the facility.

36. **LOB.** FAA Lines of Business.

37. **LOB FSMP FOCAL POINT(S).** Individuals assigned within LOB's to act as focal points for coordination with ACS in implementing the FAA Facility Security Management Program. The LOB FSMP focal point(s) may be located at the associate level in some LOB's while others may designate the office or service FSMP coordinator(s) as the focal point(s).

38. **NAS.** National Airspace System.

39. **PHYSICAL SECURITY.** That part of security concerned with the implementation of physical measures designed to safeguard personnel, to prevent unauthorized access to facilities, property, equipment, and or information, and to safeguard them against sabotage, espionage, and other criminal or terrorist threats.

40. **PHYSICAL SECURITY ASSESSMENT.** A comprehensive formal assessment of a facility's physical security program.

41. **PHYSICAL SECURITY INSPECTION.** There are two basic types of FAA inspections: comprehensive and supplemental. Physical security inspections are also an integrated part of the FSMP. Comprehensive inspections are scheduled on a regular ongoing basis to determine whether the FSMP is being implemented properly, accreditation requirements are still being met, and generally that all security protective measures are operating or functioning as required by this order. Supplemental inspections are more limited in focus and are used to determine if specific finding identified during an assessment of comprehensive inspection have been corrected.

42. **PIDS.** Perimeter Intrusion Detection System

43. PROTECTIVE BARRIERS. Physical or technical means to define the physical limits of a facility or area for the purpose of denying unauthorized access.

44. PROTECTIVE MEASURES. A physical device, person, procedure, or combination of two or more of these intended to reduce or eliminate one or more identified vulnerabilities. Protective measures are those actions taken to eliminate, reduce, or control vulnerabilities to specific threats.

45. RISK. Utilization of risk analysis techniques to identify the level of physical security protective measures are required for a facility, asset, or operation. Risk is derived by the summation of four components: Threat + Probability + Vulnerability + Criticality.

46. RESTRICTED AREA. A protected area established to control access or entry for purposes other than safeguarding classified information.

47. SABOTAGE. Any action intended to damage or destroy government property or disrupt Government operations.

48. SECURITY RISK MANAGEMENT PROGRAM. The objectives of the FAA SRM program are to ensure that the vulnerabilities and risks from all types of threats to include criminal and terrorist attack to all assets requiring safeguarding in the FAA's critical infrastructure are identified, and prioritized, and based on a logical assessment process are reduced to an acceptable level through the application of cost effective countermeasures. The FAA SRM program encompasses the entire spectrum of FAA program activity. The two largest areas of concern are the programs dealing with projects, operations, and systems, and those concerned with existing facilities, and the design and development of new facilities.

49. SET BACK DISTANCE. The minimum distance requirement from the facility to the nearest street is exterior set back. The minimum distance from the facility to the parking area is interior set back. Set back is used as a protective measure with the idea in mind that every foot between a potential bomb and a building will dramatically reduce damage and increase the survival rate.

50. SSE (SERVICING SECURITY ELEMENT). Regional (AXX-700's) and Center (AMC-700, ACT-8) Civil Aviation Security Division.

51. SYSTEMATIC PILFERER. An individual who commits theft according to a preconceived plan.

52. TERRORISM. The unlawful use or threatened use of force or violence against individuals or property for the purpose of coercion or intimidation to achieve political, religious, or ideological goals.

53. THREAT. The capability of an adversary coupled with his or her intentions to undertake any action detrimental to an asset or to the success of a program, activity, system, or operation.

54. THREAT ASSESSMENT. An evaluation of the overall threat to an asset, program, activity, system, or operation.

55. VANDALISM. Willful or malicious destruction, damage, or defacement of public and/or private property.

56. VULNERABILITY. Weakness in any aspect of an asset's design, use, mission, staffing, or other characteristic that if exploited would have an adverse impact on the security or operations of the asset.

57. VULNERABILITY ANALYSIS. The process by which facilities, operations, programs, or activities are examined to identify weaknesses susceptible to exploitation.

58. WAIVER. Temporary relief from requirements to comply with a specific standard.

APPENDIX 2. OTHER STANDARDS, LAWS, DIRECTIVES, AND ORDERS

SECTION 1. PROGRAM AUTHORITY

1. **TITLE 49, UNITED STATES CODE (U.S.C.), Section 106.** Originally Section 301(a) of the Federal Aviation Act of 1958 (PL 85-726, August 23, 1958); re-codified by PL 97-449, January 12, 1983, states that the FAA is an administration in the Department of Transportation, and covers the duties, powers, qualifications, and appointment of the Administrator and Deputy Administrator. Section 106(f) says that the Secretary of Transportation "shall carry out the duties and powers, and controls the personnel and activities, of the Administrator."

2. **49 U.S.C. SECTION 40113.** Originally Section 313(a) of the Federal Aviation Act of 1958, and previously 49 U.S.C. Appendix 1354(a). Re-codified and amended by PL 103-272, July 5, 1994. Section 40113(a), "General authority," states, "The Secretary of Transportation (or the Administrator of the Federal Aviation Administration with respect to aviation safety duties and powers designated to be carried out by the Administrator) may take action the Secretary or Administrator, as appropriate, considers necessary to carry out this part, including conducting investigations, prescribing regulations, standards, and procedures, and issuing orders."

3. **49 U.S.C. SECTION 40110,** General Procurement Authority. Originally Section 303(c) of Federal Aviation Act of 1958, and previously 49 U.S.C. Appendix 1344(c). Re-codified and amended by PL 103-272. Covers property acquisition and disposal.

4. **49 U.S.C. SECTION 44502,** General Facilities and Personnel authority. Originally Sec. 307(b) of the Federal Aviation Act of 1958, and previously 49 U.S.C. Appendix 1348(b). Re-codified and amended by PL 103-272. Section 44502(a) states that the Administrator may "acquire, establish, improve, operate, and maintain air navigation facilities; and ... provide facilities and personnel to regulate and protect air traffic."

5. **TITLE 41, CODE OF FEDERAL REGULATIONS (CFR),** Part 101-20, Management of Buildings and Grounds.

6. **COMPUTER SECURITY ACT OF 1987,** PL 100-235, enacted January 8, 1988.

7. **THE FEDERAL MANAGER'S FINANCIAL INTEGRITY ACT** (FMFIA). PL 97-255, enacted September 8, 1982.

8. **EXECUTIVE ORDER 12958,** Classified National Security Information, dated April 20, 1995.

9. **DOT ORDERS 1600.26,** Department of Transportation Physical Security Program, dated July 25, 1990, DOT Order 1500.11, and DOT Order 4410.4.

10. **NATIONAL COMMUNICATIONS SECURITY INSTRUCTION (NACSI)** Number 4008, Safeguarding Communications Security (COMSEC) Facilities, National Security Agency.

11-20. RESERVED.

SECTION 2. FAA ORDERS (*)

21. **ORDER 1000.32,** FAA Implementation of the Federal Managers' Financial Integrity Act.

22. **ORDER 1280.1,** Protecting Privacy of Information About Individuals.

23. **ORDER 1500.14,** Travel Manual.

24. **ORDER 1600.1,** Personnel Security Program.

25. **ORDER 1600.2,** Safeguarding Controls and Procedures for Classified National Security Information and Sensitive

26. **ORDER 1600.8,** Communications Security (COMSEC) and Electronic Key Management Systems (EKMS).

27. **ORDER 1600.24,** Listening-in to or Recording Conversations on Telephone or Telecommunications Systems.

28. **ORDER 1600.25,** FAA Identification Media, Official Credentials, Passports, and Vehicle Identification Media.

29. **ORDER 1600.54,** FAA Automated Information Systems Security Handbook.

30. **ORDER 1600.55,** Reporting Threats Against the President, Other Government Officials, and Visiting Dignitaries.

31. **ORDER 1600.65,** Facility Visits by Foreign Nationals and Representatives.

32. **ORDER 1650.7,** Office of Civil Aviation Security Operations Program Guidelines.

33. **ORDER 1770.11,** Mail Management Standards and Procedures.

34. **ORDER 1900.1,** FAA Emergency Operations Plan.

35. **ORDER 2770.4,** Imprest Fund.

36. **ORDER 4630.3,** Survey of Lost, Damaged, or Destroyed Government Personal Property.

37. **ORDER 4650.21,** Management and Control of In-Use Personal Property.

38. **ORDER 4650.27,** Acquisition and Distribution of Devices for the FAA Standard Key Lock System.

39. **ORDER 4770.3,** Transportation and Traffic Management of Government Property and Household Goods.

40. **ORDER 8080.6,** Conduct of Airmen Knowledge Tests.

* - The FAA orders listed here are identified by their title and order number only, without the alpha-suffix which indicates a particular version or revision. It is assumed that the current version or revision of each order is the appropriate one for reference.

APPENDIX 3. SAMPLE FORMATS, REPORTS, AND PLANS

SECTION 1. SAMPLE FORMATS[1] LISTING

[1] This sample format represents the type of information required to be consistent with this order. Future updates to this order will include specific FAA forms to accomplish this purpose.

FAA PROPERTY AND FACILITY INCIDENT REPORT-SAMPLE FORMAT

INSTRUCTIONS: All entries must be completed or marked unknown or not applicable (N/A)

1. ADMINISTRATIVE DATA

a. Reporting Facility	b. Facility Phone	c. Date Of Report
d. Location	e. Name, Title, and Telephone Number Of Reporting Person	

2. DESCRIPTION OF INCIDENT

a. Type of Incident (e.g., theft, loss, vandalism, fire, etc.)	b. Specific Incident Location
c. Date / d. Time	e. Discovered By Whom

f. Air Traffic Outage: Yes☐ (If Yes, Describe) No☐

g. Brief Narrative of Circumstances

3. IDENTIFICATION OF LOST, STOLEN OR DAMAGED PROPERTY

a. Description (model number, size, quantity, bar code, etc.)	b. Serial #
	c. Estimated Value of Loss or Damage

4. NOTIFICATION

a. FBI Agent Notified - Name	Location	
Telephone Number	Date	Time
b. Local Police Officer Notified - Name	Location	
Telephone Number	Date	Time
c. SSE Notified - Name	Date	Time

5. ADDITIONAL ACTION TAKEN

State Action Taken

6. RECOMMENDATIONS REGARDING INCIDENT

INITIAL CHECKLIST FOR GUARD CONTRACT SECURITY REQUIREMENTS-SAMPLE FORMAT

_____ **(1) Contractor's Guard Manual For FAA Facilities** (Must be reviewed and coordinated by SSE).

(2) Contractor's Suitability Investigation
(Copies of or a written summary of <u>each</u> of the following must be submitted.)

_____ Police Check
_____ 5 Year Employer Check

_____ **(3) Certification of Physical Qualification** (FAA Supplied Form)

_____ **(4) SF-85P, Questionnaire for Public Trust Positions**

_____ **(5) FD-258, Fingerprint Cards - Must submit 2**

(6) Certification of Citizenship (One of the following must be submitted.)

_____ Birth Certificate
_____ U.S. Passport .
_____ Certificate of Naturalization
_____ Report of Birth Abroad of Citizens of the U.S.

(7) Certification of Education (One of the following must be submitted.)

_____ High School Diploma
_____ GED Equivalent

_____ **(8) Proof of Minimum Age** (Driver's License, Birth Certificate, Diploma)

_____ **(9) Formal Training as Required by State.** Written certification of completion of required training must be contained in each guard's personnel file on site. (Minimum requirements include training in the following subjects: jurisdiction and authority, first aid, emergency responsibilities, knowledge of orders, security and contingency situations, safety, facility access control procedures, communications, and report writing.)

_____ **(10) Firearms Qualification** (Submissions must include score; date of qualification; "pass or fail; name, address, and telephone number of qualifying authority")

_____ **(11) Adherence to appendices 12 and 13.**

INITIAL CHECKLIST FOR GUARD CONTRACT SECURITY REQUIREMENTS-SAMPLE FORMAT

_____ (1) **Contractor's Guard Manual For FAA Facilities** (Must be reviewed and coordinated by SSE).

(2) **Contractor's Suitability Investigation**
(Copies of or a written summary of <u>each</u> of the following must be submitted.)

_____ Police Check
_____ 5 Year Employer Check

_____ (3) **Certification of Physical Qualification** (FAA Supplied Form)

_____ (4) **SF-85P, Questionnaire for Public Trust Positions**

_____ (5) **FD-258, Fingerprint Cards - Must submit 2**

(6) **Certification of Citizenship** (One of the following must be submitted.)

_____ Birth Certificate
_____ U.S. Passport
_____ Certificate of Naturalization
_____ Report of Birth Abroad of Citizens of the U.S.

(7) **Certification of Education** (One of the following must be submitted.)

_____ High School Diploma
_____ GED Equivalent

_____ (8) **Proof of Minimum Age** (Driver's License, Birth Certificate, Diploma)

_____ (9) **Formal Training as Required by State.** Written certification of completion of required training must be contained in each guard's personnel file on site. (Minimum requirements include training in the following subjects: jurisdiction and authority, first aid, emergency responsibilities, knowledge of orders, security and contingency situations, safety, facility access control procedures, communications, and report writing.)

_____ (10) **Firearms Qualification** (Submissions must include score; date of qualification; "pass or fail; name, address, and telephone number of qualifying authority")

_____ (11) **Adherence to Appendix 13.**

Rules and Regulations Governing Public Buildings and Grounds

June 1991

Federal Property Management Regulations
Title 41, Code of Federal Regulations, Subpart 101-20.3

Authority. These rules and regulations are promulgated pursuant to Public Law 566, 80th Congress, approved June 1, 1948 (Title 40, U.S. Code 318); and the Federal Property and Administrative Services Act of 1949 (Title 63, United States Statutes at Large, 377), as amended.

Applicability (41 CFR 101-20.300). These rules and regulations apply to all property under the charge and control of the General Services Administration and to all persons entering in or on such property. Each occupant agency shall be responsible for the observance of these rules and regulations.

Inspection (41 CFR 102-20.301). Packages, briefcases, and other containers in the immediate possession of visitors, employees, or other persons arriving on, working at, visiting, or departing from Federal property, are subject to inspection. A full search of a person and any vehicle driven or occupied by the person may accompany an arrest.

Admission to property (41 CFR 101-20.302). Property shall be closed to the public during other than normal working hours. The closing of property will not apply to that space in those instances where the Government has approved the after-normal-working-hours use of buildings or portions thereof for activities authorized by Subpart 101-20.4. During normal working hours, property shall be closed to the public only when situations require this action to ensure the orderly conduct of Government business. The decision to close the property shall be made by the designated official under the Occupant Emergency Program after consultation with the buildings manager and the ranking representative of the Law Enforcement Branch responsible for protection of the facility or the area. The designated official is defined in § 101-20.003(g) as the highest ranking official of the primary occupant agency, or the alternate highest ranking official or designee selected by mutual agreement by other occupant agency officials. When property, or a portion thereof, is closed to the public, admission to this property, or a portion, will be restricted to authorized persons who shall register upon entry to the property and shall, when requested, display Government or other identifying credentials to the Federal Protective Officers or other authorized individuals when entering, leaving, or while on the property. Failure to comply with any of the above applicable provisions is a violation of these regulations.

Preservation of property (41 CFR 101-20.303). The improper disposal of rubbish on property; the willful destruction of or damage to property; the theft of property; the creation of any hazard on property to persons or things; the throwing of articles of any kind from or at a building or the climbing upon statues, fountains, or any part of the building, is prohibited.

Conformity with signs and directions (41 CFR 101-20.304). Persons in and on property shall at all times comply with official signs of a prohibitory, regulatory, or directory nature and with the lawful direction of Federal Protective Officers and other authorized individuals.

Disturbances (41 CFR 101-20.305). Any loitering, disorderly conduct, or other conduct on property which creates loud or unusual noise or a nuisance; which unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways, or parking lots; which otherwise impedes or disrupts the performance of official duties by Government employees; or which prevents the general public from obtaining the administrative services provided on the property in a timely manner, is prohibited.

Gambling (41 CFR 101-20.306). Participating in games for money or other personal property or the operating of gambling devices, the conduct of a lottery or pool, or the selling or purchasing of numbers tickets, in or on property is prohibited. This prohibition shall not apply to the vending or exchange of chances by licensed blind operators of vending facilities for any lottery set forth in a State law and authorized by section 2(a)(5) of the Randolph-Sheppard Act (20 U.S.C. 107, et seq.).

Alcoholic beverages and narcotics (41 CFR 101-20.307). Operation of a motor vehicle while on the property by a person under the influence of alcoholic beverages, narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines is prohibited. Entering upon the property, or while on the property, under the influence of or using or possessing any narcotic drugs, hallucinogens, marijuana, barbiturates, or amphetamines is prohibited. The prohibition shall not apply in cases where the drug is being used as prescribed for a patient by a licensed physician. Entering upon the property, or being on the property, under the influence of alcoholic beverages is prohibited. The use of alcoholic beverages on property is prohibited except, upon occasions and on property upon which the head of the responsible agency or his or her designee has for appropriate official uses granted an exemption in writing. The head of the responsible agency or his or her designee shall provide a copy of all exemptions granted to the buildings manager and the Chief, Law Enforcement Branch, or other authorized officials, responsible for the security of the property.

Soliciting, vending, and debt collection (41 CFR 101-20.308). Soliciting alms, commercial or political soliciting, and vending of all kinds, displaying or distributing commercial advertising, or collecting private debts on GSA-controlled property is prohibited. This rule does not apply to (a) national or local drives for funds for welfare, health, or other purposes as authorized by 5 CFR, Parts 110 and 950, Solicitation of Federal Civilian and Uniformed Services Personnel for Contributions to Private Voluntary Organizations, issued by the U.S. Office of Personnel Management under Executive Order 12353 of March 23, 1982, as amended, and sponsored or approved by the occupant agencies; (b) concessions or personal nouces posted by employees on authorized bulletin boards; (c) solicitation of labor organization membership or dues authorized by occupant agencies under the Civil Service Reform Act of 1978 (Pub. L. 95-454); and (d) lessee, or its agents and employees, with respect to space leased for commercial, cultural, educational, or recreational use under the Public Buildings Cooperative Use Act of 1976 (40 U.S.C. 490(a)(16)). Public areas of GSA-controlled property may be used for other activities permitted in accordance with Subpart 101-20.4.

Posting and distributing materials (41 CFR 101-20.309). Posting or affixing materials, such as pamphlets, handbills, or flyers, on bulletin boards or elsewhere on GSA-controlled property is prohibited, except as authorized in § 101-20.308 or when these displays are conducted as part of authorized Government activities. Distribution of materials, such as pamphlets, handbills, or flyers, is prohibited, except in the public area of the property as defined in § 101-20.003(z), unless conducted as part of authorized Government activities. Any person or organization proposing to distribute materials in a public area under this section shall first obtain a permit from the building manager under Subpart 101-20.4 and shall conduct distribution in accordance with the provisions of Subpart 101-20.4. Failure to comply with those provisions is a violation of these regulations.

Photographs for news, advertising, or commercial purposes (41 CFR 101-20.310). Photographs may be taken in space occupied by a tenant agency only with the consent of the occupying agency concerned. Except where security regulations apply or a Federal court order or rule prohibits it, photographs for news purposes may be taken in entrances, lobbies, foyers, corridors, or auditoriums when used for public meetings. Subject to the foregoing prohibitions, photographs for advertising and commercial purposes may be taken only with written permission of an authorized official of the agency occupying the space where the photographs are to be taken.

Dogs and other animals (41 CFR 101-20.311). Dogs and other animals, except seeing eye dogs, other guide dogs, and animals used to guide or assist handicapped persons, shall not be brought upon property for other than official purposes.

Vehicular and pedestrian traffic (41 CFR 101-20.312). (a) Drivers of all vehicles entering or while on property shall drive in a careful and safe manner at all times and shall comply with the signals and directions of Federal Protective Officers or other authorized individuals and all posted traffic signs; (b) The blocking of entrances, driveways, walks, loading platforms, or fire hydrants on property is prohibited; and (c) Except in emergencies, parking on property is not allowed without a permit. Parking without authority, parking in unauthorized locations or in locations reserved for other persons, or parking contrary to the direction of posted signs is prohibited. Vehicles parked in violation, where warning signs are posted, shall be subject to removal at the owners' risk and expense. This paragraph may be supplemented from time to time with the approval of the Regional Administrator by the issuance and posting of such specific traffic directives as may be required, and when so issued and posted such directives shall have the same force and effect as if made a part thereof. Proof that a motor vehicle was parked in violation of these regulations or directives may be taken as prima facie evidence that the registered owner was responsible for the violation.

Explosives (41 CFR 101-20.313). No person entering or while on property shall carry or possess explosives, or items intended to be used to fabricate an explosive or incendiary device, either openly or concealed, except for official purposes. (Weapons, see Title 18, U.S. Code Section 930.)

Nondiscrimination (41 CFR 101-20.314). There shall be no discrimination by segregation or otherwise against any person or persons because of race, creed, sex, color, or national origin in furnishing or by refusing to furnish to such person or persons the use of any facility of a public nature, including all services, privileges, accommodations, and activities provided thereby on the property.

Penalties and other laws (41 CFR 101-20.315). Whoever shall be found guilty of violating any rule or regulations in this Subpart 101-20.3 while on any property under the charge and control of the U.S. General Services Administration is subject to a fine of not more than $50 or imprisonment of not more than 30 days, or both. (See Title 40, U.S. Code 318c.) Nothing in these rules and regulations shall be construed to abrogate any other Federal laws or regulations or any State and local laws and regulations applicable to any area in which the property is situated (Sec. 205(c), 63 U.S. Statutes, 390; 40 U.S. Code 486(c)).

WARNING

Title 18, United States Code, Section 930
WEAPONS PROHIBITED

Federal law prohibits the knowing possession or the causing to be present of firearms or other dangerous weapons in Federal facilities and Federal court facilities by all persons not specifically authorized by Title 18, United States Code, Section 930(c). Violators shall be subject to fine and/or imprisonment for periods up to five (5) years.

FIGURE A3-5.
PROPERTY REMOVAL RECORD Form DOT F 1660.2

DEPARTMENT OF TRANSPORTATION

Part A—To Be Completed By Each Person Removing Equipment		Date
Name (*Typed or printed*) _____ *Typed or Printed* _____ *Signature*	Description of Equipment (*Include serial number*)	Owner ☐ DOT ☐ Personal ☐ Vendor ☐ Other (*Specify*) Return date _____
Property Custodian's Name (*Printed*), Rte. Symb., Telephone No.		Property Custodians Signature Date

Part B—To Be Completed By DOT Personnel Only				
Organizational Element	Routing Symbol	Phone	Office Building	Room No.

Part C—To Be Completed By Non-DOT Personnel Only			
Employer	Address of Employer	DOT Official and Office Aware of Removal	Phone No.

Part D—To Be Completed By Guard		
Person removing property was— ☐ DOT Employee ☐ Other	If Other—Name of DOT official and office who verified removal	Verified by ☐ Phone ☐ In Person

Routing Instructions for Completed Forms

Guard: Fold original with lower third exposed, staple, and forward to security office. Provide duplicate copy to individual concerned.

Security Office: Forward to property management office.

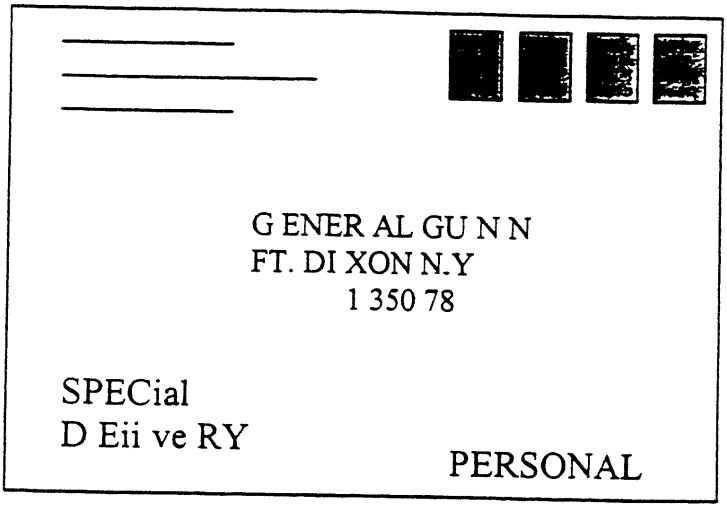
Routing of Completed Copies

To	Routing Symbol	Organization
1		
2		

Form DOT F 1660.2 (Rev. 5-91) PROPERTY REMOVAL RECORD

NO RETURN ADDRESS
Address:
- Badly typed or written
- Misspelled
- Title with no name
- Wrong title with name

EXCESSIVE OR NO POSTAGE



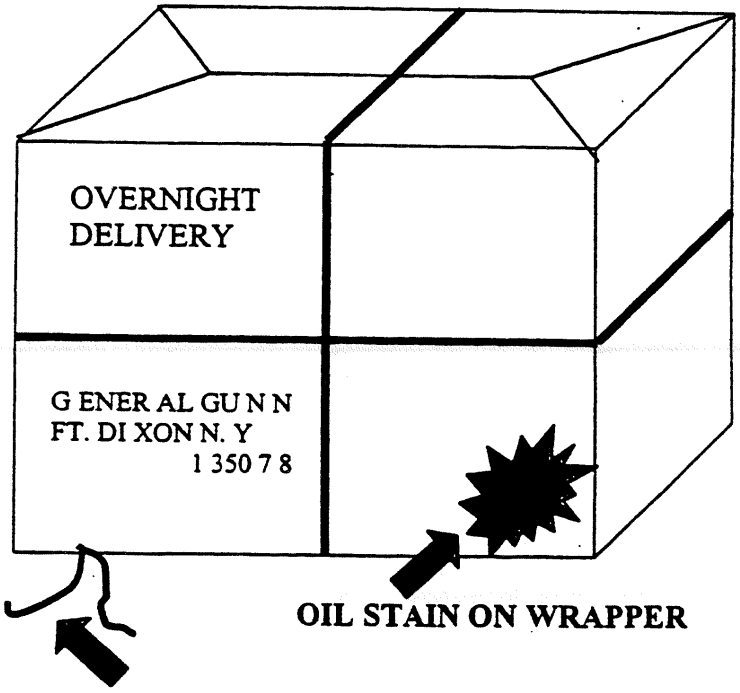
RESTRICTIVE MARKINGS

PRECAUTIONS:
1. Never accept mail, especially packages, while in a foreign country.

2. Make sure family members and clerical staff know to refuse all unexpected mail at home or office.

3. Remember - <u>IT MAY BE A BOMB</u> - Treat it as suspect.

LOPSIDED PACKAGE



OIL STAIN ON WRAPPER

PROTRUDING WIRES

APPENDIX 12. SAFEGUARDING AND USE OF FIREARMS AND CHEMICAL IRRITANTS

SECTION 1. INTRODUCTION

1. GENERAL REQUIREMENTS. Personnel, to include contract personnel, shall not be issued firearms or chemical irritants until they have been properly trained in their use and handling and there is documentation certifying their training and qualification.

2. POSSESSION OF PRIVATELY OWNED FIREARMS IN OR ON FAA-OWNED OR LEASED PROPERTY. All persons while in or on FAA-owned, FAA-leased, or GSA-leased property, including vehicles, shall comply with the following:

a. No person shall carry or have in their possession, to include their personal vehicle, firearms, or other weapons unless authorized by the FAA to do so in connection with his/her FAA official duties.

b. FAA private security guard personnel shall not carry or have in their possession firearms or other weapons except those specifically authorized in the FAA contract.

c. Firearms owned by contract security guard personnel or the security guard contractor shall not be stored on FAA property for any reason. All firearms utilized by contract security guard personnel shall be kept on the security guard's person at all times while on FAA property.

3. EXCEPTION. These prohibitions do not preclude Law Enforcement Officers on official duty. It also does not preclude FAA military (e.g. U.S Armed Forces Reservists) or civilian personnel or their dependents who reside in government-owned or leased housing from possessing firearms which are utilized for recreation or protection, providing such possession conforms to local law.

4. CARRIAGE OF FIREARMS ABOARD COMMERCIAL AIRCRAFT. Each FAA employee who is authorized to carry or transport a firearm or other dangerous weapon aboard a commercial aircraft shall fully comply with the applicable Federal Aviation Regulations (FAR).

5. PRIMARY AND ALTERNATE FIREARMS CUSTODIANS. The manager of each FAA office or element which has procured government-owned firearms and ammunition, or which intends to request such procurement, shall designate in writing a primary firearms custodian and one or more alternate firearms custodians as may be required. The primary firearms custodian, whenever possible, shall be selected from the office or element maintaining the firearm(s). The primary firearms custodian is authorized to designate the alternate firearms custodian(s) subject to the approval of the office or element manager.

a. **Records and notification.** Necessary procedures shall be established to ensure that the name, grade, job title, and duty assignment of each individual designated as primary and alternate custodian are provided in writing to the SSE and to the property officer of the servicing Logistics Division.

b. **Duties.** The custodian and, in his or her absence, the alternate custodian shall:

(1) Obtain approval for and initiate procurement requests for firearms and ammunition.

(2) Receipt for and accept custody of firearms and ammunition.

(3) Establish procedures for accountability, issuance, control, and safeguarding of firearms and ammunition in his or her custody, which include the conduct of periodic inventories, and supervision of the issuance and turn in of weapons and ammunition.

(4) Ensure compliance with the requirements of this appendix concerning issuance, physical security, and storage of firearms and ammunition.

(5) Promptly report lost or stolen firearms and ammunition to the SSE. Reference: (FAA Order 4650.21B).

(6) Report promptly to the SSE any known or suspected instances of improper safeguarding, handling, or use of firearms and ammunition.

(7) Establish safeguarding procedures to provide for secure shipment of firearms and ammunition designated for disposal, transfer, or other purposes in accordance with FAA policy.

(8) Maintain appropriate records.

(9) A custodian or alternate custodian shall not issue a firearm to an individual until the custodian has verified that the individual meets all of the criteria listed in this section.

6. ISSUANCE AND ACCOUNTABILITY. FAA employees shall be issued a government-owned firearm only when their officially assigned duties fall into categories specifically approved by the Administrator that require the employee to be armed. These categories include those listed in the following paragraphs.

7. FEDERAL AIR MARSHALS. This category includes Federal Air Marshals and such other FAA personnel who may be assigned law enforcement duties by the Administrator which specifically require the individual to be armed.

8. SURVIVAL AND EMERGENCY FIREARMS. FAA employees who are making an official flight or traveling in an operational area, such as Alaska, where Federal, state, or local authority requires that a firearm be part of the emergency survival equipment.

9. ISSUANCE OF SURVIVAL KITS. Issuance of a survival kit containing a firearm in a metal container with unbroken seal, which is carried on board an aircraft to meet the requirement identified in paragraph 25, is not considered as constructive issuance of a firearm so long as the seal is intact and the kit has not been opened. FAA personnel are required to have successfully completed an approved firearms training and qualification program to be issued survival kits containing firearms. Familiarization firing with the type of firearm contained in the survival kit is desirable and should be accomplished whenever possible.

10. ISSUANCE TO CONTRACT GUARD PERSONNEL. Issuance of government-owned firearms to private contract guard personnel is prohibited.

11. AUTHORITY. The individual must be authorized by the Administrator to carry a firearm in the performance of his/her official duties with FAA.

12. RECEIPTS. Receipts for firearms shall contain the following information:

a. Name and "ID" card number of the individual receiving the firearm.

b. Name of the issuing official (firearms custodian).

c. Office and duty assignment of the individual receiving the firearm.

d. Date of issuance and place of issue.

e. Identifying data for the firearms (serial number, manufacturer, etc.).

f. Purpose for which the firearm is issued (e.g., law enforcement duties).

SECTION 2. INVENTORY REQUIREMENTS

13. ANNUAL INVENTORY. The firearms custodian shall have an annual inventory by serial number of all firearms charged to his/her custody conducted by disinterested representatives from the Logistics or the Property Management Branch on or before June 30 of each calendar year.

14. UNSCHEDULED INVENTORIES. Irregular inventories of firearms and ammunition shall be conducted as required by appropriate Property Management and Logistics directives and may be conducted at any time by the firearms custodian and the SSE.

15. SPOT CHECK AND SPECIAL INVENTORIES. Spot checks and special inventories of firearms and ammunition shall be conducted as required by Property Management or Logistics directives, at the discretion of the firearms custodian or when so directed by the SSE.

16. CHANGE OF CUSTODIAN. Whenever there is a change of firearms custodian, a joint inventory shall be conducted of all government-owned firearms by the old and new custodian prior to the new custodian receipting for the firearms.

17. INVENTORY REPORTS. Inventory reports in writing shall be prepared by the firearms custodian at the completion of each required inventory. Format for the reports shall follow the guidelines set forth in FAA Order 4633, Physical Inventory.

18. DISTRIBUTION OF INVENTORY REPORTS. Inventory reports shall be distributed as follows:

a. Firearms custodian: one copy of current inventory for file.

b. Servicing security element: one copy of current inventory.

c. Additional copies shall be provided to the appropriate Logistics or Property Management Office as required to comply with applicable FAA directives for the element concerned.

19. INVENTORY DISCREPANCIES. Inventory discrepancies shall be reported by the firearms custodian immediately to the SSE and to the appropriate Logistics or Property Management Office.

SECTION 3. PHYSICAL SECURITY SAFEGUARDS

20. **REQUIREMENTS.** Firearms shall be stored in GSA-approved security containers at all times when not in official use.

21. **PHYSICAL SECURITY.**

a. Firearms shall be stored only in areas that have been approved by the SSE.

b. Under no circumstances will firearms and ammunitions be stored in the same security container.

c. The room in which the firearms storage container is to be located shall be of overall substantial construction.

d. The walls of the room shall extend from true floor to true ceiling if the area is not 24-hour operational.

e. The room shall, if possible, have no windows or other openings and shall meet strongroom requirements.

f. The room shall have only one entrance door of solid wood or metal construction a minimum of 1-3/4 inches thick installed using heavy-duty builders hardware throughout.

g. The door shall be hung in such a manner that the hinges are either concealed or the hinge pins are peened or spot welded to deter unauthorized removal.

h. All doors shall be secured by a high-security key actuated padlock (FSN 5340-799-8248) and associated hasp (FSN K2 5340-178-7875).

22. **INTRUSION DETECTION SYSTEM (IDS).** Each facility with a firearms storage room shall be provided with an intrusion detection system approved for that purpose by the SSE.

23. **PROTECTIVE LIGHTING.** External illumination shall be provided over all entrances to the firearms storage room or building. If the storage room has windows, lighting shall also be maintained within the storage room or building during hours of darkness to facilitate security checks.

24. **SECURITY FORCE PATROLS.** All arms and ammunition storage rooms or buildings shall be periodically checked by guards. Periodically shall be defined as a minimum of at least once per shift and will be included and described within the Facility Security Plan.

25. **SEPARATE STORAGE OF KEY FIREARMS PARTS.** Where feasible, sliding bolts or other vital parts which render small arms inoperable when removed shall be stored separately.

26. **STORAGE.** Ten handguns or less shall be stored in a GSA-approved security container of the type approved for the storage of classified information.

27. **GUN LOCKER STORAGE.** With the approval of the SSE, handguns in quantities of 10 or less, may be stored in standard gun lockers of the type approved for use by law enforcement agencies.

28. STORAGE IN QUANTITIES GREATER THAN 10. Handguns in numbers greater than 10 shall be stored in a GSA-approved, Class-5, U.S. Government Security Weapons Storage Container, equipped with a built-in, Group 1R, three position, dial-type, changeable combination lock (Reference Federal Specification AAF-36313, GSA-FAA).

29. UNAVAILABILITY OF CLASS 5 CONTAINER. When a container, such as that noted in paragraph 51 above, is not available, the following alternative safeguards shall be employed:

a. Handguns shall be stored in a GSA-approved container of the a type approved for the storage of classified security information.

b. The container shall be located in a physically secure room which has been approved for this specific purpose by the servicing security element.

30. STORAGE OF RIFLES, CARBINES, AND SHOTGUNS. Rifles, carbines, and shotguns shall be stored in a GSA-approved, Class-5 U.S. Government Weapons Storage Container, equipped with a built-in, Group 1R, three position, dial-type, changeable combination lock.

31. EXCEPTIONS TO STORAGE REQUIREMENTS. Requests for exceptions to this standard must be submitted in writing with appropriate justification through the SSE to ACO-400.

32. STORAGE. Ammunition shall be stored in a GSA-approved security container.

33. RESPONSIBILITY FOR FIREARMS CONTAINER. The firearms custodian is responsible for control of the firearms storage container.

34. STORAGE CONTAINER COMBINATION. Combinations to firearms storage containers shall be strictly controlled and safeguarded.

a. Combinations shall be changed at least once during each 12-month period.

b. Combinations shall be changed at any time that a person having knowledge of the combination is reassigned or no longer authorized access to the container.

c. Combinations will be changed when there is reason to believe that the combination has been compromised.

d. The SF-700, Security Container Information, shall be utilized to record combination changes.

35. SECURITY CONTAINER CHECK SHEET. A Security Container Check Sheet (SF 702) (NSN: 7540-01-213-7899) shall be affixed to each container and shall be filled in whenever the container is opened or locked.

36. OPEN/CLOSED SIGNS. Reversible cardboard or magnetic CLOSED-OPEN signs (GSA Supply No. 9905-286-7021 or equivalent) shall be used as additional reminders on firearms storage containers.

37. LOCKING REQUIREMENT. The firearms storage container shall be locked at all times when not in actual use.

SECTION 4. LOSS OR THEFT OF GOVERNMENT-OWNED FIREARMS

38. REPORTING REQUIREMENTS. The individual who becomes aware of the loss or theft of a firearm shall:

a. Notify the local police.

b. Notify the firearms custodian and advise him/her of the circumstances surrounding the loss or theft.

c. Notify the servicing security element if unable to reach the firearms custodian.

d. Within 24 hours from the time the loss or theft is discovered, prepare a complete written report for submission through the firearms custodian to the SSE.

39. FIREARM LOSS OR THEFT REPORT CONTENT. The report of loss/theft submitted by the individual shall be typewritten in memorandum format and shall, as a minimum, contain the following information. (See also requirements of FAA Order 4650.21).

a. Complete identifying data concerning the firearm.

b. Location where the loss or theft occurred and details of safeguards taken to protect the firearm.

c. Date and approximate time when the loss or theft occurred.

d. Time when the loss or theft was first discovered.

e. Purpose for which the firearm was originally issued.

f. Names of all persons who were with the responsible individual at the time of the loss or theft or who could provide additional information.

g. A narrative description of how the firearm was lost and/or the circumstances surrounding the theft.

h. Actions taken by the individual upon discovery of loss or theft, including notification of proper local police, etc.

40. ACTION BY THE FIREARMS CUSTODIAN. Upon receipt of a report of loss or theft of a Government-owned firearm, the firearms custodian shall:

a. Promptly inform the SSE of the loss or theft and provide complete information concerning the identifying data on the firearm.

b. Prepare a Report of Survey in accordance with FAA Order 4630.3.

41. ACTION BY THE SERVICING SECURITY ELEMENT. The SSE element upon receipt of notification that a Government-owned firearm has been lost or stolen shall:

a. Ensure that complete information concerning the lost or stolen firearm(s) has been supplied to the appropriate police jurisdiction and to the FBI.

b. Notify ACO-1 by the most expeditious means available of the loss or theft.

c. Initiate appropriate investigative activity and follow-up. Assign responsibility for the loss whenever possible and determine what administrative or disciplinary action should be taken.

d. The SSE's manager shall forward the results of the investigation to ACO-1. The manager's disciplinary action plan must be attached to the report.

SECTION 5. FIREARMS INCIDENTS

42. REPORTING OF FIREARMS INCIDENTS. All incidents involving the discharge of a firearm by an FAA employee or by a private contract security guard employed by the FAA will be reported in accordance with this section and other applicable FAA directives.

43. INDIVIDUAL RESPONSIBILITY. Each FAA employee and private contract security guard employee authorized to carry a firearm on FAA property is fully liable and responsible for actions taken involving the use of the firearm. FAA employees are specifically prohibited from using firearms in the performance of their duties except as authorized by this appendix.

44. INCIDENT REPORTING. A written report shall be rendered to the SSE any time that a firearm is discharged for any reason, whether intentionally or accidentally. This reporting requirement is mandatory regardless of whether or not personal injury resulted from the discharge.

45. PROCEDURES TO BE FOLLOWED BY THE INDIVIDUAL. The individual responsible for the discharge of the firearm shall immediately notify his/her supervisor of the incident and the circumstances relating thereto.

a. The report shall include any injury or fatality which may have resulted from the use of the firearm, including injuries resulting from accidental discharges.

b. In the event that the individual responsible is not able to initiate reporting action, it shall be the responsibility of his/her supervisor to make the report.

46. ACTIONS TO BE TAKEN BY THE SUPERVISOR. The supervisor, upon notification that a firearm has been discharged, shall take the following actions:

a. Ensure that action has been taken to notify the appropriate authorities if a fatality, injury, or damage to private property occurs,

b. Request medical aid if needed.

c. Notify the SSE by the most expeditious means available and provide a written follow-up report of the incident within 24-hours.

47. INCIDENT REPORT. The written incident report submitted by the supervisor shall contain as a minimum the following information:

a. Name and duty assignment of the individual having custody of the firearm.

b. Time of the firearm discharge (date/day/hour).

c. Reason for firing the weapon.

d. Activity in which the individual was engaged when the weapon was fired.

e. Injury, fatalities, or property damage resulting from the discharge.

f. Names of any witnesses having knowledge of the incident.

48. ACTIONS TO BE TAKEN BY THE SERVICING SECURITY ELEMENT. The FAA SSE upon notification of a firearm incident shall:

a. Notify ACO-1 of the incident and the circumstances. Notification shall include any injuries or fatalities and those agencies/authorities notified of the incident.

b. Notify the regional administrator or center or service director of the incident and the circumstances.

c. Obtain as soon as possible a written report containing full details on the discharge of the firearm. Conduct an investigation of the incident.

SECTION 6. CHEMICAL IRRITANTS

49. DESCRIPTION. Chemical irritants manufactured under various brand names, such as "mace," enable the user to exercise restraint over others. Different chemical compositions have varying degrees of hazard when improperly used. Manufacturers' instructions concerning use of the products must be understood and carefully followed.

50. RESTRICTIONS. FAA employees and contractors will comply with the local/state laws and procedures for carrying and storing chemical irritants. Additionally, the following points should be adhered to:

a. The chemical irritant shall be directed at a person at a minimum distance of 2 feet and only long enough to incapacitate the individual.

b. The chemical irritant must be aimed at the chest rather than at the face.

c. Chemical irritants shall not be used against a person who has an obvious incapacitation, has impaired breathing, or lacks normal protective reflexes.

d. A person who has been subdued with a chemical irritant must be permitted as soon as possible to wash with clear water and to use other antidotes as recommended by the manufacturer. If held in custody and adverse visual or respiratory effects continue, the individual shall be provided medical attention.

51. CROWD CONTROL. The above limitations do not apply in crowd control situations that require the use of chemical irritants as a last resort.

52. – 90. RESERVED.

APPENDIX 13. FAA CONTRACT GUARDS

SECTION 1. INTRODUCTION

1. PURPOSE. To establish minimum security standards for the selection and utilization of armed FAA contract guards for FAA facilities.

2. GENERAL. FAA contract guard personnel employed by the FAA are governed by the policies and procedures established in this appendix.

a. Use of force. Personnel duly authorized to possess or carry firearms in the performance of their duties, law enforcement, or security activities shall use only such force as is necessary to overcome any opposing force or threat by rendering the person(s) incapable of continuing the activity which prompted the use of such force or weapon.

b. Deadly force. Deadly force is authorized only when the FAA contract guard has cause to believe that another person poses an imminent threat of death or serious bodily injury to the guard or others.

c. Drawing a weapon. A firearm shall only be drawn when it is intended to be used in the protection of life.

d. Fleeing person. Firing at a fleeing person is not justified.

e. Firing from a moving vehicle. Firing from a moving vehicle or at a fleeing motor vehicle is prohibited.

f. Warning shots. Firing warning shots is prohibited.

3. FAA CONTRACTING OFFICE AND CONTRACT MONITORING REQUIREMENTS. FAA logistics, contracting offices, and contracting officer technical representatives for FAA contract guard services for FAA facilities shall:

a. Include in the contract the FAA contract guard provisions of this appendix.

b. Coordinate with the requesting office, COTR, and the SSE to ensure that the wording and provisions of contracts for FAA contract guard services comply with the requirements of this appendix prior to the contract being let.

c. Provide a copy of the contract for FAA contract guards.

d. Maintain documentation to be submitted by contractor. The following documentation shall be submitted to the Contracting Officer (CO) no less than 15 days prior to entrance on duty of a contract guard. No FAA contract guard personnel shall begin duty at an FAA facility without prior submission and a favorable review of all documentation listed below by the COTR. Copies of all documentation (reference appendix 3, figures A3-2 and A3-3) listed below shall be maintained at the facility receiving

the FAA contract guard services. The COTR shall make these records available for review by the SSE upon request.

(1) FAA contract guard certifications. Annual submission of **firearms** qualification and **medical** certifications, to include results of drug screens, are required (reference paragraphs 15, 10, and 11).

(2) FAA contract guard manual covering topics as required in paragraph 20. (2 copies)

(3) A written summary of results of contractor pre-employment investigation as required in paragraphs 13.

(4) Written certification of report of citizenship, age, and education as required in paragraphs 5, 12, and 8 respectively.

(5) Completed forms for FAA background investigation as required in paragraph 14.

FIGURE A13-1. CERTIFICATION OF PHYSICAL QUALIFICATIONS

(SAMPLE)

FEDERAL AVIATION ADMINISTRATION CONTRACT GUARDS

EMPLOYEE NAME:_____ DATE OF BIRTH:_____

ADDRESS:_____

CONTRACTOR:_____

CONTRACT NO.:_____

/ / YES / / NO The individual named has submitted to drug test/screen and has successfully passed.

/ / YES / / NO The individual listed above is physically fit to perform guard duties and is in good general health without any physical defects or abnormalities.

/ / YES / / NO The individual listed above is free of any communicable diseases.

/ / YES / / NO The individual named above possesses binocular vision correctable to 20/30 (Snellen) and is not color blind.

/ / YES / / NO The individual named possesses the capability to hear normal conversation at 20 feet and whispered conversation at 10 feet without the benefit of a hearing aid.

/ / YES / / NO The individual named above has been inoculated for immunizations to include Hepatitis A and B.

CERTIFIED BY: _____

Contractor

_____ _____

Physician Signature Date

_____

Address

_____

Phone No.

SECTION 2. FAA CONTRACT GUARD REQUIREMENTS

4. GENERAL. FAA contract guards shall be armed and consist of designated persons specifically hired, organized, trained, and equipped to perform functions in support of the FAA Facility Security Management Program for the protection of personnel, assets, and facilities. The authority of FAA contract guards varies in accordance with the location and ownership of the facility concerned and applicable local, state, and federal laws. The following basic qualifications shall apply to all individuals employed or being considered for employment as an FAA contract guards at an FAA facility.

5. CITIZENSHIP. FAA contract guards utilized by the FAA shall, without exception, be U.S. citizens.

6. PERSONAL TRAITS. The statement of work, request for bid, and any contract between the FAA and a provider of FAA contract guard services shall make it clear that each contract guard assigned to duties at an FAA facility will be expected to:

a. Exercise good judgment.

b. Interact with people in a positive manner.

c. Maintain a high level of performance.

d. Input security related data in security computer systems.

7. TRAINING. The contractor shall certify in writing to the FAA Contracting Officer (CO) that all FAA contract guards assigned duties at FAA facilities have successfully met all state and local security officer training requirements prior to assignment at an FAA facility. In addition, FAA contract guards shall have successfully completed facility and other training specified by the FAA contracting office. If there is no state or local mandated training, all FAA contract guard personnel shall be initially trained, at a minimum, in the following categories:

a. Care of Firearms. FAA contract guards will comply with all firearms certification and proficiency training requirements in accordance with this appendix.

b. Use of Firearms. Firearms will be used only in extreme emergencies requiring the protection of life and then only in accordance with the established requirements.

c. Jurisdiction and Authority. Training sessions shall include descriptions of the FAA contract guards responsibilities and authority with respect to apprehension, search, seizure, and use of deadly force.

d. First Aid. FAA contract guard personnel will be qualified in first aid and cardio pulmonary resuscitation.

e. Emergency Responsibilities. FAA contract guards shall demonstrate proficiency in the use of emergency equipment such as fire extinguishers and water hoses.

f. Operational Instructions. FAA contract guards will be able to demonstrate knowledge of the facility's: general, special, and temporary orders; facility security plan (FSP); as well as the FAA contract guard manual.

g. Security and Contingency Situations. FAA contract guards will be able to recognize and appropriately react to emergency situations involving work place violence, bomb threats, sabotage, terrorism, hostage situations, and other criminal activity.

h. Safety. FAA contract guards will be able to demonstrate general knowledge of the safety requirements for the facility with special emphasis on any volatile materials stored within the confines of the facility.

i. Facility Access Control Procedures. Training will incorporate facility guidelines and procedures for personnel and vehicle access control.

j. Communications. Training will address and allow FAA contract guard personnel to demonstrate the proper use of primary, alternative, and emergency communications equipment.

k. Reports. Training will address and allow FAA contract guard personnel to demonstrate adequate report writing skills associated with security guard force operations.

8. EDUCATION EXPERIENCE. FAA contract guard personnel shall, as a minimum, possess a high school education diploma or equivalent GED certificate and have two 2 years of experience demonstrating the ability to:

a. Meet and deal with the general public.

b. Read, understand, and apply printed rules, detailed orders, instructions and training material.

c. Construct and write clear and concise but accurate and detailed reports.

d. Maintain poise and self-control under stress.

9. WRITING AND COMMUNICATION SKILLS. The contractor shall certify in writing to the FAA CO that each FAA contract guard is fluent in speaking, reading, writing, and understanding written reports, orders, guidelines, and instructions in English and is able to write official reports in English that are grammatically correct and technically accurate.

10. PHYSICAL TRAITS. Prior to any FAA contract guard assuming duties at an FAA facility, and every year thereafter, the CO shall require positive evidence from the security guard contractor that the individual contract guard employee has passed a mandatory drug test, examined by a licensed medical doctor, and determined to be physically fit for duty to perform the normal duty functions of an FAA contract guard. The initial physical and drug test must be completed within 30 days of submission of the written certification to the CO. In addition to the requirements stated herein, the examination shall cover, as a minimum, the following:

a. An evaluation as to whether the individual is in good general health, without any physical defects or abnormalities which would interfere with job performance.

b. A determination that the individual is free of any communicable disease.

c. A determination that the individual possesses binocular vision correctable to 20/30 (Snellen) and is not color blind.

d. A test of hearing capability to determine if the individual is able to hear normal conversation at 20 feet and whispered conversation at 10 feet without the benefit of a hearing aid.

e. Provide inoculation for immunizations to include Hepatitis A and B.

(Note: If state or local medical qualifications standards for security officers are higher than those indicated above, the state and local standards shall apply.)

11. PHYSICAL FITNESS REPORT. Before assuming duties, the contractor shall certify in writing to the FAA CO, or designated representative, that each FAA contract guard has been medically examined and drug tested/screened and determined to satisfactorily meet the medical qualification requirements for FAA contract guards. These requirements shall apply to both the initial medical certification prior to beginning employment and for required annual medical certifications thereafter. The certification shall be submitted to the CO no less than 15 days prior to entrance on duty of a contract guard. The initial certification is required. The results of a mandatory drug test/screening test shall be part of the annual physical fitness report.

12. EMPLOYMENT CONSIDERATION. To be considered for employment as an FAA contract guard, each individual must be at least 21 years of age at the time of employment.

13. CONTRACTOR PRE-EMPLOYMENT INVESTIGATION.

a. Suitability Investigation. The FAA contract guard contractor providing guard personnel for assignment to an FAA facility shall be required to certify in writing to the FAA CO that each guard has successfully passed a pre-employment suitability investigation in accordance with FAA Order 1600.1, before the guard is assigned to the FAA facility.

b. Scope Of Investigation. The FAA contract guard contractor shall be required to conduct or have conducted a suitability –type investigation for each individual to be assigned security guard duties at an FAA facility. The investigation shall include the following:

(1) Search of police files in the area of residence.

(2) Inquiries of former employers for a period of 5 years.

(3) Information that may reflect on the suitability of the contract guard to perform security duties under this contract.

c. Results Of Investigation. The FAA contract guard contractor shall provide the results of the investigative reports for each contract guard to the FAA CO not later than 10 days prior to beginning duty as an FAA contract guard. The CO shall consult with the SSE and jointly disapprove an individual if the contractor's investigation is incomplete or fails to provide evidence of the guard's suitability for performing guard duties specified herein.

14. PERSONNEL AND INDUSTRIAL SECURITY REQUIREMENTS. All FAA contract guards shall be subject to an FAA National Agency Check (NAC). The contract guard contractor shall submit completed applications for this investigation to the CO not later than 10 days prior to beginning duty as an FAA contract guard. FAA Order 1600.1D Personnel Security Program, Appendix 9, Investigating Contractor Employees, provides FAA policy relating to personnel and industrial security requirements.

a. In order to protect the security interests of the government, and those transportation industry activities releasing proprietary information to FAA, all contractor employees assigned to perform service under this contract will as a minimum be the subject of a favorably adjudicated NAC.

b. Investigations will be accomplished through the FAA representative at no cost to the contractor. The logistics contracting office shall obtain an original Standard Form 85P, Questionnaire for Public Trust Positions, and two Standard Form FD-258, Fingerprint Cards, for each required check. The contractor employee must date and sign both copies of the Standard Form 85P. The completed forms are submitted to the local security office at least 10 days prior to reporting for duty. The CO shall maintain copies of the FAA contract guards facility clearance and investigations on file.

c. In the event derogatory/adverse suitability information is developed as a result of these investigations, the FAA CO shall comply with FAA Order 1600.1, Personnel Security Program, appendix 9, paragraph 10.

d. Investigative information developed by the government on contractor employees is releasable only in accordance with applicable regulations. Information relating to the national security is only releasable to individuals with a valid need to know and appropriate levels of access.

e. Classified Contract Guard Contracts. Access to classified national security information is not normally required in the performance of FAA contract guard contracts. Where classified guard contracts are required, the provisions outlined in FAA Order 1600.1 shall be followed.

SECTION 3. FAA CONTRACT GUARD FIREARMS QUALIFICATION AND CERTIFICATION

15. FIREARMS QUALIFICATION REQUIREMENTS. FAA contract guard firearms qualification shall, at a minimum, occur annually and within 12 months of the previous qualification. Qualification shall be with the identical firearm (by serial number) that will be used during regular tour of duty.

a. Range qualification shall be accomplished on a recognized law enforcement or other approved range under the supervision of a certified firearms instructor.

b. Each qualifier shall both wear and use the duty gear that is assigned for daily use. This is to specifically include the holster and reloading devices or aides (e.g. speedloaders).

c. The course of fire for FAA contract guards shall be the same as the GSA/FPS qualification course, Federal Law Enforcement Training Center Practical Pistol Course described in Figure A13-1, FAA Contract Guard Firearms Qualification Course of Fire.

16. FAA CONTRACT GUARD CERTIFICATION. FAA contract guard certification shall be in writing and must specifically state by name for each FAA contract guard:

a. The FAA contract guard has successfully completed firearms qualification within the preceding 12 months, list the score attained, the model and serial number of the qualifying weapon, and the date of qualification.

b. The FAA contract guard contractor and the FAA contract guard have fully and successfully complied with **all** training requirements of this appendix that pertain to FAA contract guard personnel.

FAA contract guard contractors shall **not** issue a firearm to their FAA contract guard employee until the contractor has certified in writing to the FAA contracting officer's technical representative (COTR) that the individual has successfully completed the firearms qualification and training (section 2, paragraph 7) requirements.

17. FAILURE TO COMPLY WITH CERTIFICATION REQUIREMENTS. FAA contract guards that fail annual certification requirements or do not comply with certification requirements shall be immediately removed from official FAA guard duty and **not be authorized** to carry a firearm until they again successfully meet all certification requirements and the FAA contract guard contractor provides certification documentation to that effect and is accepted by the FAA contract guard COTR.

FIGURE A13-1. FAA CONTRACT GUARDS FIREARMS QUALIFICATION COURSE OF FIRE

Target: NRA B-27 Silhouette; Total Shots: 60; Possible Score: 300; Minimum Passing Score: 210

DISTANCE	STAGE	POSITION	ROUNDS	SHOTS	TIME	DESCRIPTION
3 YDS	1	STANDING	6	2	3 SEC	Point shoulder, two handed, without sights
7 YDS	1		12	1	3 SEC	One shot in three seconds for the first five shots fire sixth, unload; reload with six and fire seventh, weak hand only (20 seconds allowed for reload drill). Then one shot in 3 seconds weak hand only for the "aimed in" position for the remainder of stage 1.
7 YDS	2		12	2	4 SEC	Two shots in four seconds for the first four shots. Fire fifth and sixth, unload reload with two and fire seventh and eighth (15 seconds allotted for reload drill). Load with four and holster. Then two shots in four seconds for the remainder of stage 2.
15 YDS	1		12	2	5 SEC	Two shots in five seconds for the first for shots. Fire fifth and sixth, unload, reload with six and fire seventh and eighth (25 seconds allotted for reload drill). Then two shots in five seconds for the remainder of stage 1.
25 YDS	1	BARRICADE (right)	6	2	7 SEC	Two shots in seven seconds from the right side, double action, strong hand supported by the weak.
25 YDS	2	BARRICADE (left)	6	2	7 SEC	Two shots in seven seconds from the left side, double action, strong hand supported by the weak.
25 YDS	3	KNEELING	6	2	8 SEC	Two shots in eight seconds (Kneel for each of two shots).

Note: Scoring with the NRA B-27 Silhouette target, all scores shall be based on the following conversions: (X, 10, 9, and 8 rings count as 5), (7 ring counts as 4), and (all other hits on silhouette count as 3). Hits on the white space inside arms are scored same as black areas.

SECTION 4. FAA CONTRACT GUARD OPERATIONS

18. GENERAL REQUIREMENT. Operating instructions to the facility's FAA contract guards shall be issued in writing by the FAA office exercising managerial control. Instructions to the FAA contract guards issued by the FAA contract guard contractor will be approved by the FAA COTR.

19. FAA CONTRACT GUARD ORDERS. Instructions shall be specific to the facility receiving the FAA contract guard services and be in the form of general, special, and/or temporary orders. They should be clear, concise, and fully describe the duties and actions that the FAA contract guard is to carry out under specified conditions at all individual posts. The FAA COTR will be responsible for ensuring that such orders are developed, maintained, and are current.

a. General Orders. Instructions which concern the FAA contract guard as a whole and are applicable at all posts and patrols. They will cover such items as performance of contract guard duties and responsibilities (reference paragraphs 24 and 25).

b. Special Orders. Instructions which prescribe the responsibilities of a particular post or patrol. Each post or patrol will have special orders issued concerning the location, duties, hours staffed, etc.

c. Temporary Orders. Instructions which are issued for a short period covering a special or temporary situation.

20. CONTRACTOR RESPONSIBILITY FOR FAA CONTRACT GUARD MANUAL. The FAA contract guard contractor shall be required to develop and issue a current and comprehensive FAA contract guard manual to each contract guard assigned to duty at an FAA facility. The manual is intended to be a contractor-employee manual and will contain the basic guidance issued by the contractor to its contract guard employees concerning matters of dress, discipline, patrolling, first aid, emergency responsibilities, apprehension of suspects and arrest powers, courtesy, communications, chain of command, etc. The manual shall be coordinated with the FAA COTR and the SSE before issuance.

21. WATCH CLOCK SYSTEM. FAA facilities employing FAA contract guard personnel shall provide a watch clock system or some type of electronic guard tour system to serve as a supervisory control and check on the performance of FAA contract guards.

22. CONTRACT GUARD SUPERVISOR. The FAA contract guard contract shall require the contractor to have a qualified supervisor personally check contract guard performance bi-weekly during each contract guard shift. The date and time of the supervisory visit shall be noted in the FAA contract guard log.

23. FAA CONTRACT GUARD EQUIPMENT. The FAA contract guard contract shall require that the contractor providing FAA contract guard services to an FAA facility furnish all necessary equipment required by their contract guard employees to perform their duties in a competent, capable, and efficient manner.

24. EQUIPMENT REQUIREMENTS. Minimum FAA contract guard equipment requirements include the following:

a. Only upon successful completion of the required firearms qualification and compliance with certification requirements shall a firearm, by serial number, be furnished by the contractor to each

contract guard and supervisor for duty use at an FAA facility. Only the weapon that the contract guard has qualified with shall be permitted to be used. Personal weapons shall not be used.

b. Firearms shall only be a .38 caliber, 4" barrel, standard police service type revolver. Other types of weapons loaded with .38 caliber ammunition will not be acceptable as a substitute for the requirement for a .38 caliber, 4" barrel, standard police service type revolver.

c. Firearms maintenance shall be performed on a weekly basis, or more frequently if weather conditions require to ensure optimum operating condition. The contractor shall provide all needed cleaning supplies for this function.

d. Modifications to issued firearms are not permitted with the exception of hand grips and sights. Qualification must be performed with the alteration in place and not simply removed and added before and after each qualification.

e. The FAA contract guard contractor shall provide a list of serial numbers of firearms to be used or stored on the premises to the COTR prior to the contact performance date. This list shall be kept current.

f. Ammunition for authorized firearms shall be provided by the FAA contract guard contractor. Each contract guard, entering on duty, including the uniformed on-site supervisor(s), shall be issued twelve (12) rounds of .38 caliber 125 grain hollow point ammunition. Six (6) rounds shall be used as a firearm load with six (6) rounds carried in a cartridge case. Ammunition shall be inspected and cleaned daily to ensure its safe and effective use.

g. 100 rounds of .38 caliber ammunition shall be provided by the contractor and stored on site in a lock box acceptable for storage and availability to FAA contract guards to accommodate emergencies and to be available in the event additional services are ordered.

h. All FAA contract guard personnel will wear prescribed uniforms. Deviations are not acceptable other than may be necessary in the interest of health and safety. High standards of personnel appearance will be maintained at all times.

i. The FAA contract guard contractor shall make the following typical equipment available to FAA contract guard personnel to perform normal FAA contract guard function: first aid kits, high power flashlights, key control containers, spare ammunition security container, portable communication devices (e.g. radios, wireless phones, etc.) portable fire extinguishers, traffic control devices, and such other items as the FAA may deem necessary.

25. FAA CONTRACT GUARD RESPONSIBILITIES. The contract security guard force at an FAA facility is to serve as management's representative in the administration and enforcement of the facility security program. To do this effectively, each member of the guard force must understand his or her role and responsibilities. The COTR in coordination with the SSE will provide site-specific FAA contract guard requirements for incorporation into the contract statement of work, FAA contract guard orders, and FAA contract guard manual as appropriate.

26. ITEMIZED GENERAL RESPONSIBILITIES. The following is a representative listing of general duties and responsibilities that are assigned to FAA contract guard personnel at FAA facilities.

a. Guard and protect all public and private property within FAA contract guard jurisdiction to include material, equipment, supplies, and buildings against damage, theft, fire, trespass, or sabotage.

b. To the extent specified in the contract guard contract, and as implemented in special requirements and guidelines issued by the FAA COTR, safeguard and protect all government classified, proprietary, and sensitive information, documents, material, and equipment entrusted to the care of the FAA contact guards.

c. To the extent prescribed by established orders, policies and procedures, operate, maintain, and enforce the system of personnel identification and access controls for facility employees and visitors.

d. Consistent with authority, apprehend and detain all suspicious persons, or those who attempt to gain or do gain unauthorized access to the facility, for release to local law enforcement authorities.

e. Maintain law and order and prevent illegal acts which jeopardize the safety or security of the facility and its personnel.

f. Conduct periodic patrols of the facility grounds and buildings. Provide in writing any security deficiencies and report them in an expeditious manner to the FAA COTR or an FAA facility designated representative.

g. Make appropriate station checks using a watch clock or electronic tour system equivalent.

h. Enforce the facility rules and regulations governing control of all vehicular and personnel traffic entering the facility.

i. Maintain key control for keys to facility locks and buildings issued to the FAA contract guards.

j. Report all violations of security to the COTR, facility security representative, or designated representatives.

k. In an emergency, follow existing emergency and contingency operating procedures.

l. Enforce the established policies and procedures for controlling the removal of property and documents from the facility.

m. Monitor, assess, and respond to alarms. Investigate and report any suspicious activity in accordance with established security policies and procedures.

n. Provide written and verbal reports as required by existing policies and procedures.

o. Perform escort duties as required by security policies and procedures for the facility.

p. Conduct random personnel/vehicle inspections as directed by the facility manager and/or facility security representative(s).

q. Maintain a written duty and activities daily event log for review by the FAA COTR and/or the facility security representative.

27. GENERAL OPERATIONAL PLANNING. In developing an operational plan, which includes a provision of contract security guard services, there are basic concerns which shall be addressed. This section lists some of the areas that should be considered when determining the type, number, and organization of FAA contract guards required for a given facility.

28. PLANNING CONCERNS. The following are areas that need to be considered:

a. Existing and potential security hazards.

b. Personnel and vehicle controls required for the facility.

c. Sensitivity of the facility based on type of operations conducted or types of information and/or material present.

d. The criticality of the facility.

e. Dollar value of the facility and cost of replacement.

f. Mechanical security aids employed at the facility or which could be employed at the facility.

g. Existence of large quantities of highly volatile liquids within the facility or immediately adjacent thereto.

h. Vulnerability of the facility to outside risk factors.

i. Size of the facility to be protected.

j. Condition of the perimeter barriers and their relationship to adjoining areas.

APPENDIX 14. FAA LOGISTICS CENTER

1. **GENERAL.** The FAA Logistics Center (FAALC) is located within the confines of the Mike Monroney Aeronautical Center (MMAC). The MMAC is classified as an FAA security level 4 facility and is comprised of 62 structures on 1000 acres. The MMAC is located at the southwestern edge of Oklahoma City, Oklahoma. The site is situated on South MacArthur Boulevard from SW 54th Street to SW 89th Street, on the west side of Will Rogers World Airport. All land and many of the buildings are leased from the Oklahoma City Airport Trust. The structures vary in size from single to multi level and are utilized for a myriad of purposes including administrative, aircraft maintenance and storage, medical research, training, records storage, and logistics. In addition, the MMAC has a large employee credit union, wellness center, and child care facility. The MMAC has been partially enclosed by a standard FAA security fence. Armed security guards staff and control vehicle and pedestrian entry points. These access points are located at the north and south ends of the MMAC on MacArthur Blvd. All vehicles entering the MMAC are required to display parking decals or obtain visitor permits.

2. **OBJECTIVE.** To establish physical security standards for the protection of employees and Government assets at the MMAC FAA Logistic Center facilities.

SECTION 1. CRITICAL FACILITIES

3. FAA LOGISTIC CENTER (FAALC). The FAALC is comprised of the Logistic Support Facility (LSF), Thomas Road Storage Facility (TRF), Cable Yard, Steel Yard, Special Purpose Building, Radar Antenna Laboratory Building (RAL), and the Radar Repair Facility (ATCBI). Special security measures for the FAALC include the use of armed uniformed guards, intrusion detection devices, and closed circuit television. In addition, the mandatory display of ID media is required. The security requirements set forth in this order apply to all existing and future MMAC FAALC facilities.

4. LEVEL 4 FAALC FACILITIES.

a. The LSF is a large, cavernous, single story masonry and steel structure, which was constructed in 1958. The building contains 625 thousand square feet of usable space and has been subdivided into seven distinct areas. The LSF has undergone extensive renovation since the initial construction in 1958. The facility houses the Distribution Center, AML-1000, Product Services Division, AML-4000, Radar Division, AML-2000, and the Quality Assurance Division (AML-500). The FAALC warehouse contains the bulk of replacement parts and supplies for most FAA organizations worldwide. The value of structure and contents is estimated to exceed $1 billion. The FAALC is the major supply and repair facility for all of the FAA. The LSF is classified as NAS critical and an FAA level 4 facility.

b. The Thomas Road Facility (TRF) is located approximately 4.5 miles north east of the MMAC. The TRF is a large single story structure constructed of reinforced concrete and steel. The structure contains approximately 239 thousand square feet of usable storage space. In addition, the facility has a large fenced exterior yard for the storage of bulk reutilization and marketing materials awaiting public sale. The building was leased by the FAA as an off-site facility to store overflow material from the LSF. To lessen the impact in the event the FAALC warehouse is destroyed, duplicate NAS critical electronic systems are stored at the TRF facility. Because of the high dollar amount of the inventory, presently estimated at $153 million, and the sensitive electronic equipment, the TRWHE storage facility is NAS critical and a level 4 facility.

5. LEVEL 3 FAALC FACILITIES.

a. The FAALC Cable Yard (FAALC-CY) is located in the 6500 block of South MacArthur Blvd. on the MMAC. The FAALC-CY is a large, outside, fenced storage site, which was constructed in 1958. The storage area contains 333 thousand square feet of usable space and has been subdivided into three distinct areas. The facility is utilized for the storage of large spools of electrical cable. The Product Services Division (AML-400) uses the yard to store component overhaul materials and some antenna parts. The present estimated value of the material stored in the cable yard is $8.6 million. Collocated with the FAALC warehouse, the FAALC-CY is the main supply source of electrical cable for all FAA facilities.

b. The FAA Logistic Center Steel Yard storage facility (FAALC-STY) is located in the 6900 block of South MacArthur Blvd. on the MMAC. The FAALC-STY is a large, outside, fenced storage site, which was constructed in 1961. The storage area contains 328 thousand square feet of usable space and has been subdivided into two distinct areas. The facility is utilized by the Distribution Center, AML-1000, and the Product Service Division, AML-400, to store radar antenna components, large spools of electrical cable, wooden shipping boxes, metal containers, scrap metal, portable buildings, and large truck trailers. The present estimated value of the material stored in the cable yard is $15.5 million.

c. The Air Traffic Control Beacon Interrogator (ATCBI) "Antenna Test Range," is located approximately 1 mile south of the MMAC on South MacArthur Blvd. The site sits on the West Side of MacArthur Blvd. approximately 50 yards west in an open field. The facility consists of three single story buildings constructed of steel, aluminum, and masonry materials. In addition, there is a large partially enclosed radar antenna test tower located at the southwest corner of the facility. An additional test facility, radar transmitter tower and equipment building, are located 1,700 feet north of the ATCBI facility. The ATCBI Antenna Range Shop (Work Area 1) was constructed in 1963 and contains approximately 960 square feet in four rooms. The shop is a masonry and steel, single story, structure with windows on the east side. A large portable building has been attached to the west of the structure as additional shop space. The building is designed for, and utilized as a radar antenna test and maintenance facility. The ATCBI Antenna Test Shop (Work Area 2) is a large, single-story, metal garage type structure, containing approximately 1,140 square feet of usable space. Entry to the building is by a personnel door and/or a roll up overhead door, located on the north side of the building. The ATCBI Antenna Test Tower (Work Area 3) is a large steel tower, approximately 50 feet in height, which is used to test and calibrate radar antennas. In addition, a radar transmitter building and tower is located 1,700 feet north of the ATCBI facility. The transmitter is a part of the test range but removed from the immediate site.

d. The ARSR-3 Radar Test Shop, a subsidiary of the ATCBI complex, is a large single-story, windowless, metal building, staffed facility, which was constructed in 1990. The structure contains approximately 1,900 square feet of space in four rooms. The building is designed for and utilized as a radar maintenance and test facility.

e. The Radar Antenna Laboratory (RAL) building is located east of the FAA Logistic Center's LSF in the 6600 block of Duke Avenue on the MMAC. The RAL is a single story brick and steel structure, which was constructed in 1958. The building contains approximately 2,300 square feet of usable space and has been subdivided into three distinct areas. The RAL has undergone several renovations since the initial construction in 1958. The RAL houses the NAS Automation Section (AML-447) which includes six electronic technicians.

6. LEVEL 2 FAALC FACILITIES. There are no Level 2 FAALC facilities.

7. LEVEL 1 FAALC FACILITIES. The Special Purpose Building (SPB) is an unstaffed building located south of the FAA Logistic Center's LSF in the 7000 block of South MacArthur Blvd., on the MMAC. The SPB is a single story masonry and steel structure, which was constructed in 1988. The building contains approximately 8,400 square feet of usable space and has been subdivided into five distinct areas. The SPB is used to store hazardous material such as polychlorinated biphenyl compounds (PCB), acids, solvents, and flammable materials.

SECTION 2. PERIMETER AND EXTERIOR CONTROLS

8. FAA FACILITY SECURITY STANDARDS PERIMETER AND EXTERIOR CONTROLS. The MMAC perimeter fence and controlled entry gates protect all facilities located on the Mike Monroney Aeronautical Center (MMAC). The only exceptions will be outside storage facilities, the Cable Yard and Steel Yard. Both of these exterior storage facilities are surrounded with the FAA standard security fence and gates. The TRF is located approximately 4 miles northeast of the MMAC has a dedicated FAA approved perimeter fence and controlled entry gate.

9. PERIMETER BARRIERS

a. FAA Standard Security Fence. The MMAC will be totally enclosed by the FAA standard security fence. The fence shall meet or exceed the standards as set forth by this order.

b. Clear Zone. The standard FAA security fence shall be constructed so that an unobstructed area or clear zone is maintained on both sides of the barrier. For design and engineering purposes, the interior clear zone should be at least 20 feet (6.09 meters) in width. The outside clear zone shall be a minimum of 20 feet (6.09 meters) or greater in width.

c. When The Clear Zone Requirement Cannot Be Met. When for operational, environmental, or other reasons it is not practical to establish the required clear zone, the SSE shall coordinate with the facility manager to develop compensatory measures. The SSE will evaluate the risk and vulnerability associated with the fence and recommend appropriate countermeasures which may include increasing the height of portions of the fence, providing increased lighting in the affected areas, CCTV surveillance cameras; installation of PIDS; and/or additional guard patrols, etc.

d. Gate Entrances. The number of perimeter gates, which are designated for active use, shall be kept to the absolute minimum required for MMAC operations.

e. Unattended Gates. Perimeter gates that are not manned shall be securely locked at all times. Protective lighting shall be provided to deter attempts at tampering during the hours of darkness. PIDS and CCTV protective measures shall be used when determined by the SSE to be necessary to meet safeguarding requirements.

f. Perimeter Warning Signs. FAA warning signs identifying facilities as critical to air safety and warning against trespass or attempts to damage the facility shall be affixed to the MMAC perimeter FAA standard security fence. The warning signs shall be spaced at intervals of at least 50 feet or closer if required.

10. PROTECTIVE LIGHTING. The objectives of protective lighting are to:

a. Discourage or deter attempts at entry by intruders during hours of darkness.

b. Increase the probability of detection of attempts at intrusion.

c. Permit the identification and inspection of persons and vehicles entering or departing the MMAC through designated control points.

11. ACTIVE PERIMETER ENTRANCES. Pedestrian and vehicle entrances shall be provided with two or more lighting units installed in such a way that they provide adequate illumination for recognition of persons and inspection of credentials.

12. CRITICAL ASSETS. FAALC exterior storage yards, the TRF, the Cable Yard, and the Steel Yard shall have sufficient lighting units to provide adequate illumination to protect the assets stored at these facilities.

13. PARKING LOT AREAS. FAALC parking lots shall be provided with uniform illumination of 4 – 5 foot-candles. In addition to the security hazard of providing areas of concealment, parking lots are vulnerable to pilferers and can pose a risk to employees from the standpoint of vulnerability to physical attack.

14. SECURITY GUARD GATE HOUSES. Gate houses at the FAALC facilities entrance points shall have a reduced level of interior lighting to enable the guards to see better, increase their night vision adaptability, and avoid making them a target.

15. EMERGENCY POWER. Whenever feasible, protective lighting systems at all FAALC facilities shall be connected to emergency power systems to ensure they remain operational during periods when commercial power is interrupted.

SECTION 3. VEHICLE AND PARKING CONTROL

16. SELECTION OF PARKING AREAS. Parking areas for government owned/leased vehicles by the FAALC shall be located inside perimeter fences.

17. CONTROL OF FACILITY PARKING AND VEHICLE IDENTIFICATION SYSTEM. Access to FAALC parking will be limited where possible to government and employee vehicles. Visitor and commercial parking will be offset from the FAALC facilities at least 100 feet. At a minimum, authorized parking spaces and vehicles will be assigned and identified. Procedures shall be established for identifying government and employee vehicles and their assigned parking spaces. (Placard, decal, card key, etc.)

18. POST SIGNS AND ARRANGE FOR TOWING UNAUTHORIZED VEHICLES. Procedures shall be established and implemented to alert the public and employees to towing policies and the removal of unauthorized vehicles.

SECTION 4. FAALC BUILDING CONTROLS

19. GENERAL. For FAA facilities that do not have a perimeter security fence, the exterior of the buildings shall constitute the perimeter of the facility. In these instances, the building exterior serves as both the primary and secondary lines of security safeguards. Buildings whose exterior serves as the perimeter boundary are more susceptible to unauthorized entry and compensatory measures need to be considered during the physical security assessment.

20. DOORS. Doors are an important factor in controlling entry to the facility and aid in the prevention of unauthorized access to sensitive or controlled areas.

21. NUMBER OF ENTRANCES. The number of active doors that can be used to gain access to an FAALC facility or office shall be kept to the minimum necessary to support operations. Doors, which are not essential, shall be locked or controlled by an approved access system. Doors which are identified as personnel entrances (does not include shipping and receiving dock areas) shall be located in such a way that visitors must identify themselves to a security officer before proceeding further. While all exterior doors must remain secured while not in use, they must be able to be opened from the inside for emergency exit requirements.

22. WINDOWS. Windows openings, like doors, can be inviting targets for potential intruders. They also can serve as an alternative means for removing government property and documents from a facility. Windows, like doors, have an aesthetic value and when considering security safeguards, these concerns must be addressed.

23. WINDOW SECURITY CONCERNS. Any part of a window that is 18 feet (5 meters) or less above ground or 18 feet (5 meters) or less from potential access point such as an adjoining building, tree, etc., shall be considered as vulnerable to access. Windows that are potential points of access shall be provided with locking devices, protective screens, security grills, or other appropriate safeguards to ensure that they provide an effective deterrent to their use for unauthorized or illegal purposes. In order not to corrupt the aesthetic appearance of the building, it is recommended that intrusion alarms (motion or infrared devices) be installed at or in close proximity to all windows that might provide access or forced entry points.

24. MISCELLANEOUS OPENINGS. Any opening, ventilating grills, utility grates, sewers and storm drains, building and roof openings, skylights, ventilating shafts and ducts, that provides a potential access point to a facility will require special security measures. The use of the FAA approved locking system, intrusion detection devices, bars, increased illumination, CCTV, and guard patrols is required.

SECTION 5. CRITICAL AREAS

25. GENERAL. The value and importance of the items, operations and areas to be protected, and the vulnerability of the facility will largely determine the extent of interior controls for the FAALC.

26. DESIGNATION OF FAALC CRITICAL AREAS. The following FAALC facilities are designated as critical to the NAS and the continuing operations of most FAA organizations:

a. Logistics Support Facility.

b. Thomas Road Facility.

c. FAALC Cable Yard.

27. CONTROLLING CRITICAL AREAS. The following security measures will be utilized to protect employees and visitors, control access, and protect assets at designated FAALC facilities:

a. Fixed guard posts at all active entrances of the LSF (north, east, west and south Cable Yard gate entrance and the TRF gate entrance). Exception being the shipping and receiving dock areas.

b. Effective access procedures (coded ID badges).

c. Mandatory display of ID media.

d. Use of strong rooms and cages and implemented controls for highly pilferable materials.

e. Search of hand-carried items (i.e. lunch boxes, briefcases, handbags, etc.) coming into (only when alerted by AMC-700 of a potential security risk) or out of designated FAALC facilities.

f. Use of approved locking devices.

g. Security awareness training for employees.

h. CCTV and/or IDS will be considered for unmanned gates.

i. The use of lighting systems in necessary areas.

SECTION 6. SAFEGUARDING GOVERNMENT PROPERTY

28. PROTECTION OF GOVERNMENT PROPERTY. The protection of property, including the prevention of theft, waste, and abuse of government supplies and equipment, is a mandatory responsibility for managers under the provisions of the Federal Managers' Financial Integrity Act (FMFIA), Public Law 97-255.

29. THEFT FACTORS. Actual losses due to theft depend on a number of factors, including:

a. The type, amount, and accessibility of the equipment and supplies stored at the facility.

b. The number of persons who have access to the facility.

c. Effectiveness of the property management program.

d. The adequacy of the external and internal physical security controls.

e. Employee integrity.

30. THEFT PREVENTION. The facility manager, in coordination with the SSE, shall develop the specific physical security measures that apply to reducing the vulnerability to pilferage and theft. Countermeasures recommended by the SSE include, but are not limited to, the following:

a. Security guards posted at all active entrances and exits of the LSF (north, east, west, and south Cable Yard entrance and the TRF gate entrance. Exception being the shipping and receiving dock areas.

b. Inspection of hand-carried items (i.e. lunch boxes, briefcases, handbags, etc.) coming into (only when alerted by AMC-700 of a potential security risk) or out of designated FAALC facilities.

c. Establishing an effective property removal system.

d. Investigating all thefts and losses quickly and thoroughly.

e. Monitoring high-risk storage areas with CCTV.

f. Inactive doors monitored by CCTV and intrusion detection devices.

g. Security guard patrols within and outside the facilities.

h. Random Vehicle Checks.

APPENDIX 15. CHEMICAL AND BIOLOGICAL WEAPONS

1. **PURPOSE.** We live in a rapidly changing world in which threats involving the proliferation of weapons of mass destruction and their potential use by terrorists loom over everyone. The information described below is intended to provide FAA management with assistance and guidance in understanding the concept of chemical and biological weapons. During the assessment process for new facilities, recommendations will be made for establishing safeguards dealing specifically with chemical and biological threats.

2. **AIRBORNE CONTAMINATION.** The general design strategy is to provide protected areas (toxic-free areas) and to filter all incoming air.

a. Location. Do not locate facilities in depressions. Depressions can trap contaminated air and increase the time necessary for it to dissipate.

b. Site Furnishings. Eliminate all site furnishings, vegetation, and other possible hiding places near mechanical rooms or air intakes so that perpetrators cannot use them for concealment while they introduce contaminants into the air supply. Also lay out the site to maximize opportunities for visual monitoring of the area around the facility, especially the area near the mechanical room or air intakes.

c. Airlocks. Provide airlocks at all exterior entrances and entrances to toxic-free areas. Airlocks are two-door arrangements that keep contaminated air from entering a facility when an exterior door is opened. Before the interior door is opened, the exterior door is closed and contaminated air is removed from the airlock.

d. Mechanical Room Location. Place the mechanical room on the facility exterior with an outside entrance only. This allows contaminated air filters to be removed from the facility without contaminating the interior.

e. Air Intakes. Locate air intakes on the prevailing upwind side of the facility where possible to dissipate gases quickly. Where mechanical equipment with air intake ports is roof-mounted, provide roof access from the interior of the mechanical room only or secure exterior ladders with a padlocked enclosure. Locate roof-mounted equipment as far from the roof perimeter as possible. Locate exterior air intake ports within view of occupied facilities to reduce the opportunity for a perpetrator to approach without attracting attention.

f. Wall Construction. Provide walls for the toxic-free area of reinforced concrete or reinforced concrete masonry to minimize air leakage. Treat all penetrations and intersections to make the enclosed area airtight.

g. Door Construction. At toxic-free areas, use metal doors and frames of seamless welded construction. Provide vapor seals around doors to the toxic-free areas and weather-strip all other exterior doors. Do not use louvers in exterior doors or in doors to toxic-free areas. Provide tamper resistant hinges on mechanical room doors. Provide overlapping astragals or removable mullions on pairs of doors to mechanical rooms. For paired mechanical room doors, provide a deadbolt lockset for the active leaf and a lever extension flush bolt for the inactive leaf. For single mechanical room doors, use

deadbolt locksets. Provide locks on doors into and out of the toxic-free area to prevent perpetrators from opening them to throw in contaminants.

h. Window Construction. Minimize window areas. Use only airtight inoperable windows in toxic-free areas with 1/4 inch polycarbonate glazing to prevent a perpetrator from introducing contaminants by throwing objects through the windows.

i. Roof Construction. Provide reinforced concrete roof construction to minimize air leakage and do not allow skylights. Treat all penetrations and intersections to make the enclosed area airtight. Provide a chain-link fabric enclosure a minimum of 5 feet from the top and all sides of air intakes. This prohibits thrown agents from landing directly on air intake ports and allows airborne agents to dissipate.

j. Dampers. Provide motorized dampers to close and seal intake ports when not in use. Slope sills at wall openings to prevent the placement of canisters next to openings.

k. Detection Equipment. Devices that can detect all types of chemical and biological agents in air do not exist. Each sensor type detects a different agent or a limited group of agents. In addition, many detectors are not reliable and must be manually operated. Therefore, no airborne contamination detection equipment is recommended.

l. Intrusion Detection System (IDS). Provide appropriate intrusion detection system (IDS) elements such as boundary penetration sensors on mechanical room doors to detect unauthorized entry attempts. Have the alarms annunciate within the protected facility and at a central location.

3. WATERBORNE CONTAMINATION. The general strategy is to protect the water source by restricting access, minimizing the opportunities for forced and covert entry attempts and providing bottled water for drinking.

a. Water Supply/Location. Evaluate the existing construction of the buildings for the water supply system to determine how difficult it will be to secure them against forced entry tactics. Also determine if there are any user requirements which would limit the use of bottled water for drinking. Lay out the site of the water supply system to maximize visual observation of potential locations for contaminating the water supply. Limit the number of entries to the site and lay out pathways and roads to maximize visibility. Provide means to limit perpetrator movement toward potential locations for contaminating the water supply.

b. Perimeter Barrier. Provide a standard FAA security fence around the water supply systems with gates at entry points. The fence is not a barrier to entry. It identifies a boundary and may deter perpetrators. It may also hinder perpetrators carrying heavy load of contaminants or it may facilitate visual observation of their entry.

c. Manholes. Bolt manholes with keyed bolts to prevent access to water treatment and distribution.

d. Detection of Water Contaminants. Radiological agents and most chemical agents are detectable in normal water quality testing, but biological agents frequently cannot be detected. Because water purification equipment is designed to destroy microorganisms in water, nondetection should not present a problem. Detection measures for this threat will therefore address detection and assessing perpetrators attempting to contaminate the water supply.

(1) Detection system elements. Apply IDS consisting of interior boundary penetration sensors on doors, windows, and other openings in water supply systems and storage facilities to detect unauthorized entry through openings or glass breakage. Annunciate alarms at a central control console.

(2) Access control system elements. Apply access control system elements to limit access to authorized personnel and vehicles only. Choose keyed locks, electronic card readers (electronic entry control systems), and combination-operated locks.

(3) Assessment system elements. Consider closed circuit television (CCTV) to assess IDS alarms as an option to assessment by guards. If this option is used, provide the lighting necessary for CCTV operation as well as response by facility security guards or local law enforcement.

4. AIRBORNE CONTAMINATION PROTECTIVE MEASURES CHECKLIST.

a. Facility Location. Do not locate facilities in depressions. Site the facility as far away from uncontrolled areas as possible.

b. Site Layout. Eliminate all site furnishings, vegetation, and terrain features near mechanical rooms or air intakes, which may provide hiding places. Lay out the site to maximize opportunities for visual monitoring of activities.

c. Building Layout. Establish toxic-free areas within the facility. Provide airlocks at all exterior entrances to toxic-free areas. Locate mechanical rooms on the exterior of the facility with an outside entrance only. Locate air intake ports on the prevailing upwind side of the facility. Locate air intake ports within view of occupied facilities where possible. Locate roof-mounted equipment as far from the roof perimeter as possible.

d. Walls. Provide walls for the toxic-free area of reinforced concrete or masonry to avoid air leakage.

e. Doors. Provide steel doors and frames of seamless welded construction for all doors into the toxic-free area. Provide vapor seals around doors to toxic-free areas and weather stripping for other exterior doors. Provide force entry resistant door hardware for mechanical room doors.

f. Windows. Minimize the number and area of windows in the toxic-free area. Use inoperable windows with 1/4 inch polycarbonate glazing.

g. Roofs. Provide reinforced concrete roof construction. Enclose air intakes in chain-link fabric enclosures.

h. Utility Openings. Provide motorized dampers to close air intake ports when not in use. Use slope sills at wall openings.

i. Air-Handling System. Provide a filter train with the appropriate dampers and fans in a bypass system to filter air in response to a threat. Provide the filter train described above for continuous operation.

j. Detection Measures. Provide IDS such as boundary penetration sensors on mechanical room doors.

5. WATERBORNE CONTAMINATION PROTECTIVE MEASURES CHECKLIST.

a. Site Layout. Lay out the water supply system site to maximize visual observation of activity. Limit the number of entries into the site. Lay out pathways and roads to maximize observation. Provide means to limit aggressor movement on the site.

b. Parking. Keep parking as far from potential contamination points as possible. Segregate official, employee, and visitor parking where possible.

c. Perimeter Barriers. Provide a standard FAA security fence around the water supply system with gates at entry points. (Keep entry points to a minimum)

d. Utilities. Bolt manholes shut with keyed bolts.

e. Building Elements. Provide walls and roofs of conventional construction.

f. Alternate Water Sources. Provide bottled drinking water or drinking water storage tanks in a bypass system for use in response to a threat. Provide bottled drinking water or drinking water storage tanks for continuous use.

g. Detection Measures. Apply IDS consisting of boundary penetration sensors on doors, windows, and other openings in water supply systems facilities.

h. Assessment System Elements. Provide CCTV assessment of IDS alarms.

APPENDIX 16. SECURITY CONTAINERS, VAULTS, AND STRONGROOMS

1. **SECURITY CONTAINERS.** Security containers are containers that have been specifically developed by the manufacturer and approved by GSA for the storage of classified material.

2. **CLASSES OF SECURITY CONTAINERS.** Specifications have been developed for 7 classes of security containers; however, only Classes 1, 5, and 6 are now available on the Federal Supply Schedule. Prior to selection of a particular security container, FAA managers shall coordinate with the SSE to ensure that the container selected will be adequate for their needs.

3. **CLASS 1 CONTAINER.** The Class 1 security container is insulated and comes in several models which include both a 2-drawer and 4-drawer version. Provision can be made to have more than one locking drawer to meet compartmentation requirements. The physical security protection provided by the Class 1 is expressed requirements. The physical security protection provided by the Class 1 is expressed on the test certification label as:

a. 30 man-minutes against surreptitious entry.

b. 10 man-minutes against forced entry.

c. 20 man-hours against lock manipulation.

d. 20 man-hours against radiological attack.

e. 1 man-hour against fire damage to contents.

4. **CLASS 5 CONTAINER.** The Class 5 security container offers the maximum physical security protection expressed on the test certification label as follows:

a. 30 man-minutes against surreptitious entry.

b. 10 man-minutes against manipulation of the lock.

c. 20 man-hours against manipulation of the lock.

d. 20 man-hours against radiological attack.

5. **CLASS 6 CONTAINER.** The Class 6 security container affords the same protection as the Class 5 except there is no forced entry protection. It is available in 2-, 4-, and 5-drawer models and in a map and plan cabinet. The physical security protection provided is expressed on the test certification label as:

a. 30 man-minutes against surreptitious entry.

b. 20 man-minutes against manipulation of the lock.

c. 20 man-hours against radiological attack.

d. No forced entry requirement.

6. **SAFE.** A container, usually equipped with a mounted combination lock, specifically designed for the protection of money and other highly negotiable materials or assets.

7. **BURGLARY-RESISTANT SAFES.** Burglary-resistant safes are protective storage containers designed to provide moderate to high levels of protection against both surreptitious and forced entry techniques. Depending on the specific classification of the safe, the forced entry protection ranges from attacks with common hand tools and portable electric powered tools to attacks with heavy-duty oxy-fuel cutting torches and explosives. The lower classifications of burglary-resistant safes are designed to provide protection against forced entry mainly at the door and front face of the safe. The higher classifications of safes are designed to provide forced entry protection on all six sides and can also be anchored to prevent unauthorized removal of the safe. Burglary-resistant safes are suitable for the storage of unclassified but sensitive items such as drugs, precious metals, money, or negotiable documents.

8. **CLASSES OF BURGLARY-RESISTANT SAFES.** Specifications have been developed for 5 classes of Burglary-resistant safes, TL-15, TL-30, TRTL-30, TRTL-30X6, and TRTL-60. All safes are required to have a UL listed combination lock. Prior to selection of a particular safe, FAA managers shall coordinate with the SSE to ensure that the safe selected will be adequate for their needs.

9. **TL-15 BURGLARY-RESISTANT SAFE.**

a. Weight: At least 750 pounds or anchored.

b. Body: At least 1-inch-thick steel or equal.

c. Door: At least 1-1/2-thick steel or equal.

d. Attack: Door and front face must resist attack with common hand and electric tools for 15 minutes.

e. Monetary Amount Storage: $10,000 - $50,000.

10. **TL-30 BURGLARY-RESISTANT SAFE.**

a. Weight: At least 750 pounds or anchored.

b. Body: At least 1-inch-thick steel or equal.

c. Door: At least 1-1/2-inch-thick steel or equal.

d. Attack: Door and front face must resist attack with common hand and electric tools plus abrasive cutting wheels and power saws for 30 minutes.

e. Monetary Amount Storage: $50,000 and up.

11. **TRTL-30 BURGLARY-RESISTANT SAFE.**

a. Weight: At least 750 pounds.

b. Body: At least 1-inch-thick steel with 3-inch-thick reinforced cladding or equal.

c. Door: At least 1-1/2-inch-thick steel or equal.

d. Door and front face must resist attack with tools listed above and oxy-gas cutting or welding torches for 30 minutes.

e. Monetary Amount Storage: $50,000 and up.

12. TRTL-30X6 BURGLARY-RESISTANT SAFE.

a. Weight: At least 750 pounds.

b. Attack: Door and entire safe body must resist attack with tools listed above plus electric impact hammers and oxy-fuel gas cutting or welding torches for 30 minutes.

c. Monetary Amount Storage: $50,000 and up.

13. TRTL-60 BURGLARY-RESISTANT SAFE.

a. Weight: At least 750 pounds.

b. Attack: Door and front face must resist attack with tools listed above and oxy-gas cutting or welding torches for 60 minutes.

c. Monetary Amount Storage: $50,000 and up.

Notes: TL-Tool-Resistant; TRTL-Torch and Tool-Resistant. All safes are required to have a UL listed combination lock. UL stopped issuing the TRTL-30 label, replacing it with the TRTL-30X6 label, which requires equal protection on all six sides of the safe. However, some manufacturers continue to produce safes meeting the requirements of the TRTL-30 label as specified in UL Standard 687, to satisfy the demand for moderate protection against tools and torch attack at a reasonable price.

14. VAULTS. Vaults are usually used within the FAA to store large amounts of classified material, highly sensitive material, or large size highly valuable odd-shaped or bulky components and assemblages. There are three classes of vaults: A, B, and C.

15. CLASS A VAULT.

a. **Floor and walls** shall be constructed of 8-inch thick reinforced concrete. Walls shall extend to the underside of the roof slab above.

b. **Roof shall be** constructed of monolithic concrete slab of a thickness to be determined by structural requirements but not less thick than the walls and roof.

c. **Ceiling**. Where the roof construction is not in accordance with subparagraph "b" above, a normal reinforced concrete slab will be placed over the vault area at a height not to exceed 9 feet.

d. Vault door and frame unit shall conform to Federal Specification for Class 5 vault doors.

e. Doors shall be secured by a built-in three position, Group 1R, dial-type changeable combination lock with deadbolt extension, and reinforced strike.

16. CLASS B VAULT.

a. Floor shall be of monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches (10 centimeters) thick.

b. Walls shall be of not less than 8 inches (20 centimeters) thick brick, concrete block, or other masonry units. Hollow masonry units shall be the vertical cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least 4 inches (10 centimeters) thick may be used and are required in seismic areas.

c. Roof construction shall be of monolithic reinforced concrete slab of a thickness to be determined by structural requirements but not less than 4 inches (10 centimeters) thick.

d. Ceiling. Where the roof construction is not in accordance with paragraph "c" above, a normal reinforced concrete slab shall be installed over the vault at a height not to exceed 9 feet (2.7 meters).

17. CLASS C VAULT.

a. Floor construction requirements shall be the same as for a Class B vault.

b. Walls shall be constructed of not less than 8 inches (20 centimeter) thick hollow clay tile vertical cell (double shell) or concrete block (thick shell). Monolithic steel-reinforced concrete walls at least 4 inches (10 centimeters) thick may also be used and shall be used in seismic areas. Walls back of the exterior wall of the building shall be concrete solid masonry, or hollow masonry filled with concrete and steel reinforcing bars.

c. Roof construction shall be the same as that required for Class B vault.

d. Ceiling construction shall be the same as that required for a Class B vault.

e. Vault door and frame unit shall conform to federal specifications for Class 6 vault doors.

18. STRONGROOMS. Strongrooms should be considered as an interior space enclosed by, or separated from, other similar spaces within an FAA facility by four walls, a ceiling, and a floor, all of which are normally constructed of solid building materials.

a. Under this criteria, rooms having false ceilings and walls constructed of fabrics or other similar material shall not qualify as strongrooms.

b. Facility managers shall coordinate with the SSE when considering the construction of strongrooms to evaluate the need and consider alternatives.

19. STRONGROOM CONSTUCTION REQUIREMENTS.

a. Hardware. Heavy-duty builder's hardware shall be used in construction of strongrooms. All screws, nut, bolts, hasps, clamps, bars, hinges, pins, etc., shall be securely fastened to preclude surreptitious entry and ensure visual evidence of forced entry. Hardware accessible from outside the area shall be peened, brazed, or otherwise modified in a manner approved by the SSE to make unauthorized removal difficult. Walls and ceiling construction shall be of plaster, gypsum board, metal, hardboard, wood, plywood, Number 9-guage, 2-inch wire mesh or stronger, or other material offering similar resistance to, or evidence of, unauthorized entry into the area. Insert type panels shall not be used.

b. Floor shall be of solid construction, utilizing materials like concrete, ceramic tile, wood, etc.

c. Window openings shall be fitted with 0.5 inch (1.25 centimeter) steel bars, separated by not more than 6 inches (15 centimeters) on center, with cross bars to prevent spreading spaced not more than 12 inches (30 centimeters) apart, or, Number 9-gauge security mesh fastened by bolts extending through the wall and secured on the interior side of the window frame. In addition to being kept closed at all times, the windows shall also be opaqued by any practical method, such as paint on both sides of the window, or covering the entire window opening on the inside with tempered masonite, sheet metal, plywood, etc.

d. Miscellaneous openings. Where ducts, registers, sewers, and tunnels have an area of 96 square inches (0.06 meters) or more and constitute possible points of unauthorized access, they shall be equipped with man-barriers such as Number 9-gauge wire mesh, with 2-inch (5 centimeter) square mesh or steel bars of at least 0.5 inch (1.25 centimeter) in diameter extending across their width with a maximum spacing between bars of not more than 6 inches (15 centimeters) on center. The steel bars shall be securely fastened at both ends to preclude removal with cross bars to prevent spreading.

e. Doors may be of metal construction or of solid wood construction reinforced with a metal plate on the interior side. When doors are used in pairs, an astragal (overlapping molding) shall be used where the doors meet. When the construction is of Number 9-gauge, 2-inch (5 centimeter) wire mesh, a door constructed of similar material may also be used. However, the wire mesh door shall be reinforced with a metal panel at least 36 inches (90 centimeters) wide from floor to ceiling welded to the inside of the wire mesh wall next to the FAA approved high security locking device.

f. Door louvers and baffles plates will not be used. If for some reason they have to be used they shall be reinforced with Number 9-gauge wire mesh, with 2-inch square mesh fastened to the inside of the door and covering the louvers or baffles.

g. Doors shall be secured by FAA approved built-in three position, dial-type changeable combination lock with deadbolt extension, and reinforced strike. If the strongroom construction is of Number 9-gauge, 2-inch (5 centimeter) security mesh, the locking device shall be alarmed to detect tampering with the lock. Locking device and alarm systems (where applicable) must be of a type approved by the SSE, and the installation must be inspected by the SSE before the alarm is placed into operation.

20. STORAGE OF CLASSIFIED INFORMATION. Vaults and strongrooms shall not be used for open storage of classified material, as a substitute for the security container requirements specified in FAA Order 1600.2, for the safeguarding of national security classified information, and material, without the written approval of the SSE.

21. COMBINATIONS FOR VAULTS AND STRONGROOMS. Combinations for vaults and strongrooms shall be recorded, controlled, changed, and accounted for in accordance with the requirements for safeguarding and controlling combinations contained in FAA Order 1600.2.

APPENDIX 17. SECURITY RISK MANAGEMENT (SRM) ASSESSMENT PROCEDURES FOR LEVEL 3 AND 4 FACILITIES

1. GENERAL. This appendix specifies the procedures that an assessment team should follow in preparing for and conducting an SRM assessment at a Level 3 or 4 facility.

2. PREPARATION.

a. At least 60 days prior to the assessment, the SSE or other organization responsible for the assessment team shall send a letter to the manager of the facility to be assessed and send a copy to the line of business (LOB) organization responsible for the facility. The letter shall explain the reason for the assessment and shall include the proposed dates for it, the names of the assessment team members, and proposed dates and times for the in-briefing and out-briefing.

b. The organization responsible for the assessment shall make every effort to include not only security specialists but also facility and/or LOB personnel as assessment team members.

c. The letter to the facility manager shall also request use of workspace and any equipment that the team will need during the assessment. In addition, it shall request any documents or items of information that the team wants to have prior to beginning the assessment, including:

(1) Name(s) and phone numbers(s) for point(s) of contact at the facility that will serve as a liaison with the assessment team.

(2) Copies of the facility's Occupant Emergency Plan (OEP) and any memorandum of agreement (MOA) that the facility has with a Federal, state, or local agency.

(3) Facility "as built" drawings.

(4) Copies of security training records and any waivers or exceptions to security policies pertaining to the facility.

d. Either from the facility, the LOB, or the appropriate SSE, the assessment team shall obtain information prior to the assessment about emergency services for the facility (police, fire, rescue) and the utility companies that serve it (electric power, telephone, gas, and water), along with telephone numbers and points of contact for the agencies/companies. The team shall coordinate with the SSE in obtaining as much pertinent information from these agencies/companies as possible prior to the assessment, such as information about local crime statistics. It shall also arrange with agency/company personnel for any meetings that the team wants to have while conducting the assessment.

e. The assessment team shall coordinate as appropriate with LOB organizations to obtain information about facility and/or environmental changes that have occurred since the last survey or inspection. In addition, the team shall review previous surveys and/or inspections of the facility, which are available in the Facility Security Reporting System (FSRS).

f. The assessment team shall try to obtain as much information and do as much coordination as possible in advance of the actual assessment in order to lessen the amount of time that it has to spend at

the facility. The SSE, the facility, and the LOB shall fully support the team in its efforts to obtain documents and information and to coordinate with outside agencies/companies in advance.

g. The assessment team shall ensure that all equipment necessary for the assessment, such as a laptop computer and a camera, is available and in working order.

3. CONDUCTING THE ASSESSMENT.

a. The assessment team should begin the assessment with an in-briefing to the facility manager and his/her staff. In this briefing, the team should briefly explain the assessment process and how it differs from a traditional survey or inspection, emphasizing that facility and/or LOB personnel need to be fully part of the team. The team should ensure that both team members and facility personnel understand what the team will be doing and what assistance it will need from facility personnel. The team members should also mention findings of the last previous survey or inspection, address any other topics that the manager or the team would like to discuss, and arrange a specific time for the out-briefing.

b. The team shall conduct the assessment as specified in appendix 18. The team members shall interview facility personnel, review available records, meet with emergency services and utility company officials, and observe all areas of the facility as needed to obtain all necessary information.

c. In the out-briefing, the assessment team, including those team members who are facility and/or LOB personnel, shall provide the facility manager and his/her staff all pertinent information about its findings. The team members should discuss the facility's critical assets and associated risks, vulnerabilities, existing countermeasures, and recommended countermeasures. They should also mention possible administrative actions that would reduce risk. In addition, the team should explain that the report it prepares will be provided to the LOB.

d. As soon as possible after completing the assessment, the team shall compile its data and prepare the assessment report. It shall include in the report all pertinent information about the facility's critical assets, asset values and risk levels, vulnerabilities, and existing and recommended countermeasures.

APPENDIX 18. SECURITY RISK MANAGEMENT (SRM) ASSESSMENT PROCESS FOR LEVEL 3 AND 4 FACILITIES

1. **PURPOSE.** This appendix describes the steps in the SRM assessment process for Level 3 and 4 facilities. In this process, the assessment team compiles quantifiable data to help determine not only essential elements of risk to these facilities, but what measures the agency should take to reduce to an acceptable level those risks that are unacceptable. The assessment results help management to identify what countermeasures are most cost-effective and to decide how best to utilize resources.

SECTION 1. PROCESS STEPS

2. IDENTIFY CRITICAL ASSETS. Section 2 contains lists of critical assets normally found at Level 3 and 4 facilities.

3. DETERMINE CRITICALITY RATING.

a. The assessment team should assign each asset a numerical rating from "1" to "4" based on impact of loss. Both the operational impact and the financial cost of the loss of the asset affect the criticality rating. The most critical assets receive a rating of "1," while the least critical ones receive a rating of "4." Figure A18-1 lists the criticality ratings and defines each based on impact of loss.

FIGURE A18-1. CRITICALITY RATINGS BASED ON IMPACT OF LOSS

Criticality Rating Severity of Loss	Impact Description Level of Impact	Impact of Loss
1	Catastrophic	Total destruction of loss of the asset or damage to the asset sufficiently severe to cause complete loss of mission capability for an extended period.
2	Very serious	Major damage to the asset requiring extensive repairs with consequent severe impairment of the mission capability.
3	Moderately serious	Damage to the asset is sufficient to require immediate repairs with noticeable impact of the capability of the facility to accomplish its mission.
4	Not serious	Damage to the asset is such that there is no noticeable adverse impact on the capability of the facility to perform its mission.

b. The financial cost of loss is the total of the following:

(1) Cost of a permanent replacement. These costs include, as appropriate, purchase price or manufacturing cost, freight and shipping charges, and costs for site preparation, installation, testing, and activation.

(2) Cost of a temporary substitute. It may be necessary to install a substitute asset while waiting for a permanent replacement. The costs of this substitute may include lease or rental costs and the costs of labor, testing, and activation.

(3) Repair costs, if damage to the asset is repairable.

(4) Total lost revenue cost; i.e., resources diverted from other projects to meet emergency needs due to loss of the asset.

(5) Total related costs. These costs include those of waiting or downtime for other personnel or systems as a result of the loss.

c. When two or more assets receive the same criticality rating based on impact of loss, those with the potentially greater financial loss should receive a higher priority for protection.

d. Section 2 contains typical replacement costs for critical assets at various Level 3 and 4 facilities.

4. IDENTIFY THREATS ASSOCIATED WITH EACH ASSET. This process incorporates elements of a traditional threat assessment, in that it includes any information or data about the probability that a particular threat will occur. After identifying the asset, the assessment team shall consider what threats may result in a loss event for a particular asset.

a. The following are examples of possible threats:

(1) identifying the insider (disgruntled employee) and outsider (organized crime or hate groups) threats, civil disturbances,

(2) attacks using explosives (including blast,) letter or package bomb, domestic terrorism, or arson,

(3) unauthorized physical or electronic access, technical surveillance,

(4) assault, sabotage, theft of government property, espionage, inappropriate disclosure, vandalism.

5. IDENTIFY AND ASSESS EXISTING COUNTERMEASURES.

a. Countermeasures are those actions taken to eliminate, reduce, or control vulnerabilities to specific threats. In many instances countermeasures require funding.

b. The assessment team shall identify existing countermeasures and determine the extent to which they are providing the intended vulnerability reduction. Section 3 provides a list of possible existing countermeasures.

c. The assessment team shall also review the functional security requirements in section 4 to help determine whether or not the existing countermeasures are providing the necessary degree of risk reduction.

6. ASSIGN EACH ASSET A VULNERABILITY RATING.

a. The assessment team should evaluate each asset, previously placed in priority order (paragraph 3), to determine the extent to which it is vulnerable to the identified threats. Vulnerabilities are those physical, technical, administrative, procedural, or human characteristics of an asset that constitute quantifiable weaknesses. If a threat occurs, these weaknesses increase the probability that it will be successful in causing damage to or loss of an asset.

b. The level of risk associated with an asset is directly related to the magnitude of the vulnerabilities. The greater the number and magnitude of vulnerabilities, the greater is the probability or risk that damage or loss will occur. Vulnerabilities are a measure of the probability of loss.

c. The assessment team shall assign an alphabetical rating from "A" through "D" to each asset to show the vulnerability or probability of loss level. The "A" rating designates the highest level of vulnerability and the "D" rating the lowest, as shown in figure A18-2 below.

FIGURE A18-2. VULNERABILITY AND PROBABILITY OF LOSS RATINGS

	Rating	Description --
Certain	A	Given no changes the threat or loss event will occur.
Highly Probable	B	The threat or loss event is much more likely to occur than not to occur
Moderately Probable	C	The threat or loss event is more likely to occur than not to occur.
Improbable	D	The threat or loss event is less likely to occur than not to occur.

7. USE RISK LOGIC MATRIX AS A TOOL TO HELP MANAGE RISKS.

a. The assessment team should combine the criticality rating (level of impact) and the vulnerability rating (probability of loss) to obtain the risk level for each asset. It should then group the assets according to criticality and vulnerability and report the results. The SSE and the LOB should then work together to develop an effective method for utilizing resources to effectively manage risk.

b. The risk logic matrix, Figure A18-3, Risk Logic Matrix, provides a clear perception of the critical decision boundaries. Assets with a risk level of 1A, 1B, 1C, 2A, 2B, or 3A are commonly referred to as falling within the "red zone."

FIGURE A18-3. RISK LOGIC MATRIX

		Impact of Loss			
Assessed Rating	Probability of Loss	1 Catastrophic	2 Very Serious	3 Moderately Serious	4 Not Serious
A	Certain	1A	2A	3A	4A
B	Highly probable	1B	2B	3B	4B
C	Moderately probable	1C	2C	3C	4C
D	Improbable	1D	2D	3D	4D

c. The term managing risk is significant. The entire thrust of the security risk management process is to provide a logical and comprehensive set of procedures for determining where management must spend resources to reduce unacceptable risks. It also helps management understand what options exist in directing resources to protect assets in the remaining risk categories. Management can apply this process equally effectively to any asset when its value in terms of impact of loss can be quantified. When the process has been completed to the stage where the risk logic matrix is complete, the decision maker can readily identify those vulnerabilities (1A, 1B, 1C, 2A, 2B, 3A) that have the highest priority for elimination or control because of the serious or catastrophic consequences of the impact of loss.

d. The risk matrix management guide, Figure A18-4, Risk Matrix Management Guide, shows which asset risk levels are unacceptable and must be controlled or eliminated; which ones should be unacceptable, but which management may decide to accept, and which ones management may accept with proper review. There are three guides, incorporating the threat as being high, medium, or low in probability as determined by the assessment team.

FIGURE A18-4. RISK MATRIX MANAGEMENT GUIDE

HIGH THREAT	
FAA Asset Risk Level	Interpretation
1A, 1B, 1C, 2A, 2B, 3A	These risks are unacceptable and must be controlled or eliminated.
1D, 2C, 2D, 3B, 3C	These risks are unacceptable and must be controlled or eliminated.
3D, 4A, 4B, 4C, 4D	These risks should be unacceptable. However, management may determine to accept the risk in writing.
MEDIUM THREAT	
FAA Asset Risk Level	Interpretation
1A, 1B, 1C, 2A, 2B, 3A	These risks are unacceptable and must be controlled or eliminated.
1D, 2C, 2D, 3B, 3C	These risks should be unacceptable. However, management may determine to accept the risk in writing.
3D, 4A, 4B, 4C, 4D	These risks may be accepted with management review.
LOW THREAT	
1A, 1B, 1C, 2A, 2B, 3A	These risks should be unacceptable. However, management may determine to accept the risk in writing.
1D, 2C, 2D, 3B, 3C	These risks may be accepted with management review.
3D, 4A, 4B, 4C, 4D	These risks may be accepted with management review.

e. LOB managers responsible for FAA facilities shall use the most cost-effective measures possible to address the risks in priority order and to reduce the vulnerabilities associated with unacceptable risks to an acceptable level.

f. Risk reduction measures (countermeasures) include physical modification, procedural changes, or other measures that will reduce the level of risk to an acceptable level. Managers shall ensure that risk reduction strategies include measures that meet the functional security requirements similar to those listed in section 4 and shall consider all appropriate countermeasures and their associated costs. Section 5 lists the countermeasures (with estimated costs) that managers should consider.

8. CONDUCT A COST BENEFIT ANALYSIS.

a. In applying the SRM assessment process, security specialists and LOB personnel quantify all of its essential elements in terms of dollars. Following an SRM assessment, the security team and

managers shall conduct a cost benefit analysis in evaluating potential risk reduction strategies. The analysis will then assist the manager in determining the advantages and disadvantages of alternative approaches to a given risk reduction situation and weighing the comparative costs of each risk reduction option.

b. Section 6 contains the specific procedures for a cost benefit analysis.

SECTION 2. LIST OF CRITICAL ASSETS

This section lists assets normally found at various Level 3 and 4 facilities and their typical replacement costs. When conducting a security risk management assessment, an assessment team may use it to check those assets that a particular facility actually has and to record criticality and vulnerability ratings.

FIGURE A18-5. AIR ROUTE TRAFFIC CONTROL CENTER

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Personnel		2.7M X's No. Personnel		
Main ARTCC Building		$35,000,000		
Annex Building		$1,000,000		
AAS NCO Building		$200,000		
WECO 300 Switch		$2,240,000		
Enhanced Direct Access Radar Channel (EDARC)		$2,050,000		
Voice Switching and Control System (VSCS)		$62,000,000		
Peripheral Adapter Module Replacement Item (PAMRI)		$786,000		
Master DEMARC		$1,157,000		
Operations Control Room Equipment		$2,000,000		
Critical Power Buss and Switching Room		$1,000,000		
Central Computer Complex Host (CCCH)		$14,000,000		

FIGURE A18-5. AIR ROUTE TRAFFIC CONTROL CENTER (cont.)

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Chiller Equipment		$6,000,000		
Day Care Center		$1,500,000		
UPS Power Conditioning, and Generator Building and Equipment		$13,100,000		
Computer Display Channel (CDC)		$2,499,000		
Radio Communications Link (RCL)		$2,800,000		
Cooling Towers		$200,000		
Maintenance Processor Sub-system (MPS)		$1,678,000		
Traffic Management Unit (TMU)		$142,000		
National Airspace System Data Interchange Network (NADIN 1A) Node		$200,000		
National Airspace System Data Interchange Network (NADIN II) Node		$200,000		
Flight Data Input Output System (FDIO)		$122,000		
Satellite Dish (List Type)		$100,000		
Satellite Dish (List Type)		$100,000		
Satellite Dish (List Type)		$100,000		
Flight Service Data Process-ing System (FSDPS)		$700,000		
MWP Weather Antennas		$50,000		
Recovery Communications Spira Cone Antenna		$150,000		
Leased Interfacility NAS Communication System (LINCS)		$500,000		
Radio Control Equipment (RCE)		$2,500		
Data Multiplexing Network (DMN)		$8,774,000		
Backup Emergency Commu-nications (BUEC)		$3,704		
VSCS Demarc		$62,000,000		

FIGURE A18-6. LEVEL 5 AIR TRAFFIC CONTROL TOWER CRITICAL ASSETS

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Personnel		2.7M X's No. Personnel		
ATCT Building		$21,360,000		
Critical Power		$1.000,000		
Master DEMARC and (LINCS)		$1,000,000		
DBRITE		$516,000		
Remote Transmitters/Receivers (RTR)		$125,000		
Fiber Optics		$1,896,000		
Chillers		$40,000		
ASDE		$100,000		
ILS		$10,000		
RVR		$240,000		
DVRS		$150,000		
ASOS		$350,000		
ATIS		$6,000		
DASI		$24,000		
LLWAS		$342,000		
FDIO		$59,000		

FIGURE A18-7. COMBINED ENROUTE RADAR APPROACH CONTROL AND INTERNATIONAL FLIGHT SERVICE STATION CRITICAL ASSETS

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Personnel		$2.7M X's Personnel		
CERAP Operations Building		$15,000,000		
Mechanical Building		$1,000,000		
Administrative Building		$4,750,000		
Technical Support Building		$1,500,000		
EARTS		$17,000,000		
CERAP Control room		$2,000,000		
Master DEMARC		$500,000		
ICSS		$1,000,000		
Critical Power System (Gen., UPS, & PCS)		$4,650,000		
Chiller		$2,000,000		
Water Treatment System		$150,000		
Cooling Towers		$200,000		
Radio Communication Link (RCL)		$2,800,000		
AFSS Model 1		$1,000,000		
LINCS		$1,000,000		
Satellite Antenna		$100,000		

FIGURE A18-8. TERMINAL RADAR APPROACH CONTROL CRITICAL ASSETS

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Personnel		$2.7M X's No. Personnel		
Main TRACON Building		$14,463,166		
ARTS – III		$1,000,000		
Master DEMARC		$1,150,000		
Critical/Emergency Power		$1,000,000		
Back-up Engine Generator		$62,000		
UPS Equipment		$95,000		
Cooling Tower		$100,000		

FIGURE A18-9. NATIONAL NETWORK CONTROL CENTER CRITICAL ASSETS

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Personnel		2.7M X's No. Personnel		
NNCC Building		$3,500,000		
NADIN II (PSN)		$2,500,000		
Band-Width Manager (BWM)		$150,000		
LINCS Equipment		$66,131,000		
TELCO DEMARC		$240,000		
NADIN I		$80,000,000		
WMSCR		$30,000,000		
AWP		$560,000		
System Data		$162,000,000		
Environmental Controls		$1,500,000		
Uninterrupted Power Supply		$150,000		

FIGURE A18-10. AIR ROUTE SURVEILLANCE RADAR/JOINT SURVEILLANCE SYSTEM CRITICAL ASSETS

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Telco Room				
Uninterrupted Power Supply/Power Cleanup System				
Exterior Fuel Tank				
Diesel Generator				
Operations Room				
Microwave Link				
Air Conditioning Unit				
Fixed Pole System (FPS) 6D Series				
ARSR ½ or				
Model 3				
Model 4				
Beacon System				

FIGURE A18-11. AIR TRAFFIC CONTROL SYSTEM COMMAND CENTER CRITICAL ASSETS

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Personnel		2.7M X's No. Personnel		
Main ATSCC Building		$35,000,000		
WECO 300 Switch		$2,240,000		
Enhanced Direct Access Radar Channel (EDARC)		$2,050,000		
Voice Switching and Control System (VSCS)		$62,000,000		
Peripheral Adapter Module Replacement Item (PAMRI)		$786,000		
Master DEMARC		$1,157,000		
Operations Control Room Equipment		$2,000,000		
Critical Power Buss and Switching Room		$1,000,000		
UPS Power Conditioning, and Generator Building and Equipment		$13,100,000		
Computer Display Channel (CDC)		$2,499,000		
Radio Communications Link (RCL)		$2,800,000		
Maintenance Processor Subsystem (MPS)		$1,678,000		
Traffic Management Unit (TMU)		$142,000		
National Airspace System Data Interchange Network (NADIN 1A) Node		$200,000		
National Airspace System Data Interchange Network (NADIN II) Node		$200,000		
Flight Data Input Output System (FDIO)		$122,000		
Satellite Dish (List Type)		$100,000		
Satellite Dish (List Type)		$100,000		

FIGURE A18-11. AIR TRAFFIC CONTROL SYSTEM COMMAND CENTER CRITICAL ASSETS (cont.)

Asset	Chk	Replacement Cost	Criticality	Vulnerability
Satellite Dish (List Type)		$100,000		
Flight Service Data Processing System (FSDPS)		$700,000		
MWP Weather Antennas		$50,000		
Recovery Communications Spira Cone Antenna		$150,000		
Radio Control Equipment (RCE)		$2,500		
Backup Emergency Communications (BUEC)		$3,704		

SECTION 3. EXISTING COUNTERMEASURES

This section lists existing countermeasures normally found at various Level 3 and 4 facilities. When conducting a SRM assessment, an assessment team may use it to check those countermeasures that a particular facility actually has.

FIGURE A18-12. EXISTING COUNTERMEASURES CHECKLIST

Countermeasures	Facility Currently Has
Perimeter barrier:	--
Fence	
Height	
Top guard	
Vehicle Gate(s)	
Pedestrian Gate(s)	
Concrete and/or steel composition barrier	
Perimeter signage	
Guard rails	
Alternate barrier	
Access Control:	
Agency photo ID displayed above waist at all times	
Government Employees	
Contractors	
Visitors	
Vendors	
Vehicle Registration	
Vehicle Inspection Area	
Key control	
Access/proximity card control	
Agency standard Best locks	
Visitor control/screening system	
Visitor ID accountability system	
Establish ID issuing authority	
Prevent unauthorized access to utility/critical areas	
Critical or restricted areas identified, posted, and access controlled	
High risk property secured and access restricted	
Conduct background checks and/or establish security control procedures for service contract employees	
Guard Force:	
Supervisor	
Armed (security officer)	

FIGURE A18-12. EXISTING COUNTERMEASURES CHECKLIST (cont.)

Countermeasures	Facility Currently Has
Unarmed (security guard)	
Guard House (booth)	
Patrol	
Watch tour or form of official recording	
Posts (location and hours)	
Lighting:	
Perimeter	
Parking	
Building/exterior	
Parking:	
Control of facility parking	
Control of adjacent parking	
Post signs and arrange for towing of unauthorized vehicles	
ID system and procedures for authorized parking	
Handicapped parking	
Adequate number of spaces	
Monitored	
CCTV:	
Camera:	
Color Camera (w/lens/bracket)	
Color Camera (w/pan/tilt/zoom lens)	
Black and White Camera (w/lens/bracket)	
Black and White Camera (w/pan/tilt/zoom lens)	
Camera Housing	
Video Recorder	
CCTV Switcher	
Monitor(s)	
Central monitoring	
Time lapse video recording	
Post signs advising of 24 hour video surveillance	
IDS:	
Perimeter	
Interior	
Exterior	
Sensitive areas (critical assets)	
Central monitoring	
Shipping and Receiving:	
Procedures established	

FIGURE A18-12. EXISTING COUNTERMEASURES CHECKLIST (cont.)

Countermeasures	Facility Currently Has
x-ray screening of all packages	
Magnetometer	
Occupant Emergency Plan (OEP):	
OEP in place, updated and tested at least annually	
Assign and train OEP personnel	
Day Care Center:	
On facility compound	
Off facility compound	
Law Enforcement (LE):	
Establish liaison with local, state, and federal LE agencies	
Attend monthly/quarterly LE liaison meetings	
Memorandum of Understanding on file for:	
Police	
Fire (hazardous material)	
Emergency Services (medical)	
Utilities (water, electrical, telephone)	
Training:	
Conduct annual security refresher training	
Conduct annual tenant training	
Train OEP officials	
Establish unarmed guard qualifications/training requirements	
Establish armed guard qualifications/training requirements	
Intelligence:	
Review/establish procedures for intelligence receipt and dissemination	
Establish uniform security/threat nomenclature	
BLAST (for new/design facilities):	
Install mylar on all exterior windows (7 millimeters)	
Parking-100ft. standoff distance for a 50 lb. Bomb	
Perimeter-300ft. standoff distance for a 1000lb. Bomb	
Review current projects for blast standards	
Review/establish uniform standards for construction	
Review/establish new design standards for blast resistance	
Emergency power:	
Provide emergency power to critical systems	

SECTION 4. FUNCTIONAL SECURITY REQUIREMENTS

To reduce vulnerability to criminal and violent activity, all Level 3 and 4 facilities shall employ countermeasures to meet functional security requirements. Listed below are some examples of such requirements:

1. All parking shall be at least 100 feet from the facility.

2. The facility shall have a minimum distance of 300 feet between the perimeter barrier and any part of the facility. The perimeter barrier and gates shall have a design and engineering goal to stop a 5-ton vehicle traveling at 35 miles per hour. Existing facilities shall have perimeter intrusion detection and access control systems that will identify any attempt by unauthorized persons to circumvent the authorized access procedures or perimeter barrier.

3. The perimeter barrier should serve as a deterrent or delay to unauthorized trespass by personnel. In the event that unauthorized physical access is attempted, the perimeter barrier should provide a positive alarm or other indication to a response force.

4. Access through the perimeter barrier gates shall require the presentation of a valid credential to a sensor reader or a security officer.

5. A security risk management system shall include 24-hour CCTV surveillance and time lapse video monitoring as part of an integrated system.

6. The facility shall have a central security control center for all interior and exterior CCTV and access control systems and equipment.

7. The facility shall have a trained, well-equipped security officer staff to operate the control center and to respond to emergencies and alarms. The security officer(s) shall have equipment that will enable them to communicate with the security control center and to communicate during emergencies.

8. The perimeter barrier shall define the property line and control the flow of vehicles and personnel to designated entry points.

9. The design and engineering of the perimeter must be such that perimeter barriers and gates will stop a vehicle weighing 5 tons, traveling at a speed of 35 miles per hour.

SECTION 5. RISK REDUCTION MEASURES

This section lists countermeasures that a facility may install or employ to reduce or eliminate vulnerabilities and reduce the level of risk. It also shows typical costs for many of these countermeasures. An SRM assessment team may use this section to compute the total costs of countermeasures when conducting a cost benefit analysis.

FIGURE A18-13. RISK REDUCTION MEASURES

Description	Cost	Annual Cost	Total
Access Control:			
Agency photo ID			
Government Employees			
Contractors			
Visitors			
Vendors			
Vehicle Decal			
Badge clips			
Badge chains			
Badge pouch			
Vehicle Inspection Area			
Key control			
Access/proximity card			
High security lockset w/reinforced strike plate			
Critical or restricted areas signs			
Conduct background checks for service contract employees			
Security Control Center 20x20 @ $1.00 sq. ft.			
IDS:			
Central monitoring			
Cable			
Perimeter barrier:			
Fence 7 ft.			
Fence 7 ft. w/1 ft. topguard			
Fence 7 ft. w/1 ft. topguard w/PVC coating			
Jersey barrier			
High security vehicle gate w/supporting systems			

FIGURE A18-13. RISK REDUCTION MEASURES (cont.)

Description	Cost	Annual Cost	Total
Drop arm vehicle barrier w/support system			
Protective bollards			
Pedestrian Gate(s)			
Concrete and/or steel composition barrier			
Perimeter signage			
Guard rails			
Guard Force:			
Supervisor			
Armed (security officer)			
Unarmed (security guard)			
Guard House (booth)			
Patrol			
Watch tour or form of official recording			
Lighting:			
Perimeter 20 ft. steel pole set in concrete			
Building/exterior			
Parking:			
Post signs			
ID system and procedures for authorized parking			
CCTV:			
Color Camera (w/lens/bracket)			
Color Camera (w/pan/tilt/zoom lens)			
Black and White Camera			
Black and White Camera (w/pan/tilt/zoom lens)			
Weatherproof enclosure			
Video Recorder w/time lapse, date/time feature			
CCTV Switcher w/12 camera capacity			
Monitor 19 inch digiplex w/control			
Central monitoring			
Fiber optic cable in conduit			

FIGURE A18-13. RISK REDUCTION MEASURES (cont.)

Description	Cost	Annual Cost	Total
Post signs advising of 24 hour video surveillance			
Shipping and Receiving:			
Procedures established			
x-ray machine			
Magnetometer			
Occupant emergency plan (OEP)			
Training:			
Annual security refresher training			
Conduct annual tenant training			
Train OEP officials			
Unarmed guard training			
Armed guard training			
BLAST (for new/design facilities):			
mylar (7 mil)			
Emergency power:			
Provide emergency power to critical systems			

SECTION 6. COST BENEFIT ANALYSIS (CBA) PROCESS

This section explains the process for conducting a CBA.

CBA Formula:

1. Total cost of critical assets. (See section 2.) Cost may or may not include personnel.

2. Percent of Risk Reduction (Based on any functional security requirements for the facility, such as those shown in section 4, that a recommended countermeasure would affect. For more detailed explanation, see the sample CBA below.).

3. Multiply number 1 by number 2.

4. Gives cost benefit of _____.

5. Divide benefit of by cost of risk reduction measure (See section 5.).

6. The result is the cost benefit ratio.

Sample CBA:

Facility: Terminal Radar Approach Control Center (TRACON).

Facility personnel: 112. Number on site during normal daytime shift: 42

Value of 42 personnel, at $2.7 million each (from section 2): $113,400,000

Other critical assets at facility: Main building, critical/emergency power supply,

ARTS III, Master DEMARC, engine generator, UPS, and cooling tower.

Total replacement cost for the critical assets: $17,870,166

Recommended countermeasure: Intrusion Detection System (IDS)

Cost of recommended countermeasure: $50,000 (from section 5)

Functional security requirements: Refer to sample list in section 4. Assume for this exercise that all nine of the requirements apply at this facility and that all are of equal value; i.e., each would be worth approximately 11 percent of the total.

The IDS would meet two of the nine functional security requirements. The total percent of risk reduction in this example would be 22 percent, or two times 11 percent.

The formula would then work in this manner:

Without considering personnel:	Considering personnel:
1. $17,870,166	1. $131,270,166
2. 2 X's 11% = 22%	2. 2 X's 11% = 22%
3. Multiply 1 X 2 ='s	3. Multiply 1 X 2 ='s
4. $3,931,436	4. $28,879,436
5. $3,931,436 divided by $50,000	5. $28,879,436 divided by $50,000
6. Equals 78.628 which rounded equals 79 to 1	6. Equals 577.588 which rounded equals 578 to 1

For every dollar spent on the intrusion detection system, there would be $79 of *economic* value, or a ratio of 79 to 1 without considering personnel ($577 of *economic* value, or a ratio of 577 to 1, if personnel are included). Although the economic value is very favorable, the security value is not because the IDS would only reduce the risk by 22 percent and would require other risk reduction measures to bring the level of risk within an acceptable level.

APPENDIX 19. THE FAA BLAST STANDARD AND DESIGN GUIDELINE

1. FAA BLAST STANDARD

a. Applicability. This appendix shall be used when evaluating the protection level for all new FAA facility designs, considered for new leased office buildings, and where applicable for existing facilities due to special circumstances, such as major retrofits or construction.

b. Threats. The detonation of an explosive device results in airblast overpressures (blast), shrapnel, and shock loadings. All three explosive effects must be considered. The following minimum explosive threat levels shall be used in the design phase of all FAA facilities or as a special consideration for an existing facility.

(1) Exterior Attack (1,000 pounds TNT). The primary threat is a 1,000 pounds TNT equivalent explosive device delivered by vehicle (stationary or moving) to the perimeter of the FAA site.

(a) In order to minimize the consequences of such an attack with minimum hardening of the facility, a minimum 300-foot set-back distance is required.

(b) Even with the minimum set-back distance, some hardening of the facility may be required.

(2) Exterior Attack (50 pounds TNT). The secondary threat is a 50 pounds TNT equivalent explosive device delivered by hand or by vehicle interior to the site perimeter but exterior to the protected facility.

(a) This threat applies to on-site parking areas.

(b) A minimum set-back distance of 100 feet is required between the bomb and the facility.

(c) As with the 1,000 pounds threat, even with the minimum set-back distance, some hardening of the facility may be required.

2. DESIGN AND PLANNING REQUIREMENTS FOR BLAST

a. Blast resistant designs, analyses, and assessments for FAA design phase facilities shall be performed and/or reviewed by qualified personnel.

b. Proper structural dynamics analysis methods shall be employed in blast resistant design. The analysis and design shall take into account the various loading conditions based on the needs of each project.

c. Design engineers shall be responsible for submitting to the national program manager a design narrative and copies of design calculations at each design phase which identify the building specific response to the protective criteria when measured against the blast standard.

d. Requirements for blast resistance in FAA structures shall be integrated into the overall building design starting with the planning phase. Reasonable and prudent measures shall be taken to:

(1) Minimize the extent and severity of potential injuries.

(2) Control the potential damage to facilities and prevent collapse.

(3) Control the impact on mission capability to within acceptable limits.

3. METHODS AND REFERENCES FOR BLAST. All building components requiring blast resistance shall be designed using established methods and approaches for determining dynamic loads and dynamic structural response.

4. BLAST CONSIDERATIONS FOR NEW DESIGNS AND LEASED OFFICE BUILDINGS. The following design guidelines apply to both new FAA facility designs and newly leased office buildings.

a. Facility designs which are vulnerable to progressive collapse from natural or human-related incidents must be avoided. At a minimum, all new FAA facilities and new leased office buildings shall be designed for the loss of one primary vertical load-bearing member. This shall be located at the building perimeter for the first two floors above grade without progressive collapse.

b. New facility designs shall be designed with a reasonable probability that, if local damage occurs, the structure will not collapse or be damaged to an extent disproportionate to the original cause of the damage.

c. In the event of an internal explosion, the design shall prevent progressive collapse due to the loss of one primary vertical load bearing structural member. The designer may show how the proposed design precludes such a loss if another method is chosen.

d. All building materials and types are allowed which are also acceptable under model building codes. Special consideration shall be given to materials which have inherent ductility and which are better able to respond to load reversals (i.e., cast in place reinforced concrete and steel construction). Careful ductile detailing is required for material such as prestressed reinforced concrete, precast concrete, and masonry to adequately respond to design loads. The most important areas of concern include exterior walls, windows and doors, roof systems (slabs and beams), and framing systems (columns and beams).

5. STRUCTURAL ENGINEERING CRITERIA FOR BLAST. The following design guidelines apply to both new FAA facility designs and newly leased office buildings.

a. Windows. Windows shall be made of shatter resistant material (e.g. polycarbonate) to protect personnel and citizens from the hazards of flying glass as a result of impact or explosion. Additional blast resistance can be achieved by using tempered or safety glass, smaller windows, and/or only constructing windows on sheltered sides of buildings.

b. Materials. Cast-in-place reinforced concrete is the preferred material for blast protection. However, properly designed and detailed steel structures may be considered. In order to economically provide protection from blast within these types of constructed facilities, inelastic or post elastic design shall be considered standard. This allows the structure to absorb the energy of the explosion through plastic deformation while achieving the objective of saving lives.

shall be considered standard. This allows the structure to absorb the energy of the explosion through plastic deformation while achieving the objective of saving lives.

c. Symmetric Design. Symmetric reinforcement needs to be taken into design consideration.

d. Balanced design of all building components is essential. For example, for window systems the frame and anchorage shall be designed to resist the full capacity of the weakest element of the system.

e. Ductile detailing shall be used for connections, especially primary structural member connections. In many cases, the ductile detailing requirements for seismic design and the alternate load paths provided by progressive collapse design assist in the protection from blast. Connections for steel construction shall be ductile and shall develop as much movement connection as practical. Connections for cladding and exterior walls to steel frames shall develop the capacity of the wall system under blast loads.

SECTION 2. SAMPLE REPORTS FORMAT LISTING

30.-39. RESERVED.

SECTION 3. SAMPLE PLANS FORMAT LISTING

FACILITY SECURITY PLAN OUTLINE[1]-SAMPLE FORMAT

Chapter 1. Overview

Section 1. General

1-1. Purpose.

1-2. Distribution

1-3. Definitions

1-4. For Official Use Only

1-5. Effective Date

1-6. Facility Mission

1-7. Responsibilities and Reporting

1-8. Delegation of Authority

1-9. Threats and Vulnerabilities

1-10. Operations Security

Section 2. Crime, Violence, and Unauthorized Activities

1-11. Purpose

1-12. General

1-13 – 1-17 (Types of Crime Violence and Unauthorized activities)

Section 3. Bomb Threats and Incidents

1-18. Telephonic Bomb Threat

1-19. Written Bomb Threat

1-20. Personal Contact

1-21. Letter and Parcel Bombs.

[1] **For electronic copies of a sample Facility Security Plan contact ACO-400.**

Chapter 2. Information Security

2-1. Information Security Plan
- a. Education, Training and Awareness
- b. Access Controls
- c. Identification and Marking
- d. In-Use Protective Measures
- e. Storage Requirements
- f. Methods of Transmittal
- g. Methods of Reproduction
- h. Destruction Methods
- i. Policy for Violations

2-2. Categories of Information Requiring Protection
- a. Classified Information
- b. For Official Use Only (FOUO)
- c. Privacy Act Information
- d. Sensitive Security Information (SSI)

Chapter 3. Automated Information Systems

3-1. Purpose

3-2. Background

3-3. Terminology and Definitions

3-4. Security

Chapter 4. Security Systems

4-1. General

4-2. Physical Devices

4-3. Mechanical Devices

4-4. Electronic Devices

4-5. Employee and Contractor Security Responsibilities

4-6. Concept of Protection In-Depth

Chapter 5. Normal Security

5-1. General

5-2. Hours of Operation

5-3. Conformity With Signs and Directions

5-4. Inspection of Purses, Briefcases, and Packages

5-5. Acceptance of Mail and Deliveries

5-6. Parking

5-7. Access Controls

5-8. Visits by Foreign Nationals and Representatives

Chapter 6. Emergency Operations

6-1. Emergency Operations

6-2. Emergency Operations Entry Control

6-3. Readiness and Security Condition Levels

6-4. Emergency Evacuation Procedures

6-5. Facility Security Preparedness Log

6-6. Emergency Contact and Notification Lists

6-7. Types of Emergencies

Appendices

Appendix 1. Occupant Emergency Plan (OEP)

Appendix 2. Emergency Contact List

Appendix 3. Security Conditions

Occupant Emergency Program

More than 900,000 people work in approximately 6,800 federally owned or leased Federal buildings. Countless visitors pass through these facilities each year. The U.S. General Services Administration (GSA) is the agency responsible for ensuring the safety and security of all of these people while they are on Federal property.

The Federal Property Management Regulations (FPMR) specifically require GSA to assist Federal agencies who occupy these facilities in establishing and maintaining asn Occupant Emergency Program (OEP). The FPMR defines an OEP as ". . . a short-term emergency response program [that] establishes procedures for safeguarding lives and property during emergencies in particular facilities."

An OEP has two components. The first is the development of procedures to protect live and property in federally occupied space under certain emergency conditions. The second is the formation of an Occupant Emergency Organization within each agency, comprised of employees designated to undertake certain responsibilities and perform the specific tasks outlined in its OEP.

NOTE: The relevant sections of the FPMR are contained within the Appendix of this booklet.

Occupant Emergency Plans

This publication provides a step-by-step guide to assist Federal agencies in meeting FPMR occupant emergency requirements. As each agency completes development of an OEP, pertinent information should be published as a directive entitled *Occupant Emergency Plan for (Name of Facility)* and copies distributed to all individuals responsible for action in the event of an emergency.

The published Occupant Emergency Plan directive should contain a sign-off sheet, similar to the one on this page. Verification that those responsible for managing and performing tasks during an emergency is necessary to ensure that those individuals are aware of their responsibilities.

For small, one-level facilities, emergency information (telephone numbers, responsible individuals coordinators, etc.) may be entered on GSA Form 3415, Occupant Emergency Plan (abbreviated), shown on the following page. This form may not be used for facilities with more than 500 employees, unless its use is approved by the individual primarily responsible for the Occupant Emergency Program.

Responsible Officials' Sign-Off Sheet

By their signatures below, the following officials verify that they have participated in the development of this Occupant Emergency Plan and fully understand the procedures to be followed in an emergency affecting the facility and employees for which they are responsible.

Designated Official:
Name _____
Signature _____
Title _____

Building Manager:
Name _____
Signature _____

Tenant Agencies:
Agency _____
Ranking Official _____
Signature _____
Agency _____
Ranking Official _____
Signature _____
Agency _____
Ranking Official _____
Signature _____
Agency _____
Ranking Official _____
Signature _____

Physical Security Specialist:
Name _____
Signature _____

FIGURE A3-41.
OCCUPANT EMERGENCY PLAN—SAMPLE FORMAT

Responsibility

The FPMR places responsibility for managing emergencies in a federally owned or leased facility upon a "Designated Official," who is ". . . a designee selected by mutual agreement of occupant agency officials." (Section 101-20.003, Definitions). This person must supervise the development of the Occupant Emergency Plan and the staffing and training of the Occupant Emergency Organization.

Emergency Telephone Numbers

All personnel in the building should know who to contact in case of emergency. A list of emergency telephone numbers should be available to everyone. One way to ensure that everyone has and keeps a copy is to publish the list in the Federal telephone directory, preferably on the inside of the front cover or on the first page. The list also should be published with the Ocupant Emergency Plan for the facility. Of course, it should be updated as assignments change.

Building/Occupant Information

The Occupant Emergency Plan should contain specific information about the building's construction and its occupants in narrative form or on a Building Information Sheet and Occupant Information Sheet. Floor plans should be included, with evacuation routes clearly marked.

The Command Center

Emergency operations are directed form a Command Center. The Center should be ccentrally located and easily accessible for effective communication and control. A possible location would be the building's control center where the alarm panel is located. The Center should have good communications capability, including at least two telephones and, if possible, portable radios and pagers. Messengers should be available to augment communications systems.

Provision should be made for an alternate Command Center, in case the main one is incapaciated, and for a Command Center at the site to which employees would be transferred if the facilityhas to be evacuated.

Include the location and telephone number fo the Command Centers and alternate sites.

OCCUPANT EMERGENCY PLAN (Abbreviated) | DATE
(This form is provided as a suggested guide for storefront and/or ground level small office space)

AGENCY	MEDICAL ASSISTANCE	
FIRE	POLICE	OTHER PHONE
FEDERAL PROTECTIVE SERVICE	BUILDING MANAGER	
OFFICIAL IN CHARGE	DUTY PHONE	

EMERGENCY ORGANIZATION INFORMATION
(Coordinators, Monitors, and Bomb Search Officer)

	NAME	DUTY	OFFICE PHONE	OTHER PHONE
1.				
2.				
3.				
4.				

EMERGENCY PLAN GUIDANCE

Know Evacuation Routes — Know the Plan of Action

FIRE OR SMOKE
1. Sound building alarm.
2. Call Fire Department _____
3. Notify Official in Charge _____
4. Notify Buildings Manager _____
5. Notify Federal Protective Service _____
6. Assist Fire Department.
7. Close windows and doors (Do no lock)

EARTHQUAKE
1. Take cover under table, desk, or in doorway.
2. Do not run outdoors.

SEVERE WEATHER
1. Secure objects outside building.
2. Prepare to move to place of safety.
3. Stay away from large windows.
4. For tornado, open windows.
5. Know location of utility shutoff valves and switches.
6. Stay tuned to weather reports.
7. Standby for further instructions.

BOMB THREAT
1. Record information on back of this form.
2. Notify Official in Charge _____
3. Notify Police _____
4. Notify Federal Protective Service _____
5. Notify Buildings Manager _____
6. Search immediate area and public areas for suspicious object.
7. If suspicious package or bomb found:
   a. Do not touch.
   b. Notify Bomb Squad _____
   c. Evacuate area.

CIVIL DISTURBANCE
1. Notify official in charge.
2. Secure doors.
3. Notify Police _____
4. Notify Federal Protective Service _____
5. Notify Buildings Manager _____

NOTE: In all emergencies, be prepared to assist the handicapped.
Bomb Threat Checklist on Reverse Side

Direct orderly flow of persons during fire drills and emergencies along prescribed routes, including orderly exit from the building at the first or ground floor.

- Ensure that all persons have vacated the floor.

Area or Wing Monitors

- Work with floor monitor; notify floor monitor when area has been completely cleared.

- Ensure that evacuation routes are clearly identified and made known to occupants.

- Direct orderly flow of persons during drills and emergencies, along the prescribed evacuation routes.

- Ensure that area or wing is completely vacated, when required.

- Ensure that windows and doors are closed, lights on, and electrical appliances off during fire evacuations.

- Ensure that windows and doors are left open and light on during bomb threat evacuations.

- Supervise stairwell monitors and monitors for the handicapped; maintain list of handicapped persons, providing revisions to the floor monitor. (List should include name, telephone extension, room number, and type of handicap.)

Stairwell Monitors

- Support the area/wing monitor.

- If evacuating because of a bomb threat, search stairwell.

- Control movement of persons on stairways, keeping them in single file and moving steadily at a walking pace; instruct persons to grasp handrails.

- Keep door open to stairway until the area/wing is clear.

- Restrict and monitor use of stairwells and escalators as necessary.

- Assign monitors for the handicapped, one per handicapped person.

Floor Team/_____ Floor (continued)
(Elevator Monitors)

Combine a sheet of elevator monitor for each floor there elevator may not be captured. Buildings with automatic elevator capturing systems will need elevator monitors only for the floor where elevators are captured.

Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____
Telephone _____
Elevator _____ Monitors _____

Elevator Monitors

- Assist floor monitors.

- Be familiar with the provisions of GSA Bulletin FPMR D-198 covering emergency plans for using elevators to evacuate handicapped persons.

- Be familiar with manual operation of elevators.

- Capture assigned elevator and permit use only as directed by floor monitor.

- During fire evacuation, direct persons attempting to use elevator to appropriate stairway; relinquish control of elevator to firefighting personnel when they arrive.

- If emergency personnel are arriving by elevator, meet them and direct them to the scene of the emergency.

Communications

Of high-priority concern to members of the Occupant Emergency Organization are the primary and alternate means of communication that will be used (1) to activate the organization; (2) to inform building occupants of the nature of an emergency and what action to take; and (3) to coordinate activities during the emergency.

In some cases, the building's fire alarm system may be sufficient means of notifying the organization and the occupants. However, such a general alarm may not be available or appropriate, and telephones, public address systems, and/or messengers may prove more feasible. If telephones are used, a communications coordinator should be appointed to set up a system of contacting all members of the emergency organization. This person could also be responsible for updating lists of telephone numbers.

Multilevel buildings may have emergency telephone systems for coordinating emergency activities. However, most buildings must rely on the normal telephone system, the public address system, the fire alarm, and messengers.

Child Care Centers in Federal Facilities

The designated official and a physical security specialist should work with the director of a child care center in a Federal facility to develop and post emergency response procedures. Center staff should know whom to contact in the event of a medical emergency, how the center will be notified of a fire or other danger that may require evacuation, the location of fire alarm boxes and fire extinguishers, the primary and secondary evacuation routes, and the locations of safe areas.

Each staff member should be assigned a specific group of children for whom he or she is to be responsible during an emergency. Center staff should conduct practice drills over the prescribed evacuation routes so children will not be unprepared or unduly alarmed should a real emergency occur.

Responsible Officials' Sign-Off Sheet

By their signatures below, the following officials certify that they have participated in the development of this Occupant Emergency Plan and fully understand the procedures to be followed in an emergency affecting the facility and employees for which they are responsbile.

Designated Official:

Name _____
Signature _____
Title _____

Building Manager:

Name _____
Signature _____

Tenant Agencies:

Agency _____
Ranking Official _____
Signature _____

Agency _____
Ranking Official _____
Signature _____

Agency _____
Ranking Official _____
Signature _____

Agency _____
Ranking Official _____
Signature _____

Physical Security Specialist:

Name _____
Signature _____

Emergency Telephone Numbers

Building Command Center _____

Alternate _____ Off-site _____

Building Manager _____

Fire Department _____

Police:

Federal Protective Service _____

Local Police Department _____

Bomb Disposal:

Military _____

Local Police _____

Hazardous Materials Information:

CHEMTREC: 800-424-9300 (from Washington, DC, 483-7616)

(Also list numbers of state and local agencies, local number for Environmental Protection Agency, and poison control centers.)

_____

_____

_____

_____

Utilities:

Gas _____

Electric _____

Water _____

Telephone _____

Building Information Sheet

Building name _____

Building number _____

Address _____

_____

Year building completed _____

Type of construction _____

_____

Number of floors _____

Mezzanine(s) _____

_____

Basement(s) _____

_____

Gross floor areas _____ square feet

Net assignable floor area _____ square feet

Government occupied floors _____

_____

Other Tenants _____

_____

Fire alarm system and signals _____

_____

Automatic sprinkler system _____

Voice communications systems _____

FIGURE A3-41.
OCCUPANT EMERGENCY PLAN—SAMPLE FORMAT

OCCUPANT EMERGENCY PLAN (Abbreviated)

(This form is provided as a suggested guide for storefront and/or ground level small office space)

DATE			
AGENCY		AGENCY	
FIRE	POLICE	MEDICAL ASSISTANCE	
FEDERAL PROTECTIVE SERVICE	BUILDING MANAGER	OTHER PHONE	
OFFICIAL IN CHARGE	DUTY PHONE		

EMERGENCY ORGANIZATION INFORMATION

(Coordinators, Monitors, and Bomb Search Officer)

	NAME	DUTY	OFFICE PHONE	OTHER PHONE
1.				
2.				
3.				
4.				

EMERGENCY PLAN GUIDANCE

Know Evacuation Routes — **Know the Plan of Action**

FIRE OR SMOKE

1. Sound building alarm.
2. Call Fire Department _____
3. Notify Official in Charge _____
4. Notify Buildings Manager _____
5. Notify Federal Protective Service _____
6. Assist Fire Department.
7. Close windows and doors (Do no lock)

EARTHQUAKE

1. Take cover under table, desk, or in doorway.
2. Do not run outdoors.

BOMB THREAT

1. Record information on back of this form.
2. Notify Official in Charge _____
3. Notify Police _____
4. Notify Federal Protective Service _____
5. Notify Buildings Manager _____
6. Search immediate area and public areas for suspicious object.
7. If suspicious package or bomb found:
   a. Do not touch.
   b. Notify Bomb Squad _____
   c. Evacuate area.

SEVERE WEATHER

1. Secure objects outside building.
2. Prepare to move to place of safety.
3. Stay away from large windows.
4. For tornado, open windows.
5. Know location of utility shutoff valves and switches.
6. Stay tuned to weather reports.
7. Standby for further instructions.

CIVIL DISTURBANCE

1. Notify official in charge.
2. Secure doors.
3. Notify Police _____
4. Notify Federal Protective Service _____
5. Notify Buildings Manager _____

NOTE: In all emergencies, be prepared to assist the handicapped.

Bomb Threat Checklist on Reverse Side

TELEPHONE BOMB THREAT CHECKLIST
Important: REMAIN CALM

CODE NUMBER

SECTION I — INSTRUCTIONS

1. Follow instructions received from your supervisor, Federal Protective Officer, or the designated official.

2. If you are ordered to evacuate, take with you any drafts, forms, or reports you may have prepared regarding the threat.

SECTION II — PERTINENT DATA

1. TIME BOMB IS SET TO EXPLODE

_____ a.m. _____ p.m.

2. DESCRIBE TYPE OF BOMB

4. LOCATION OF BOMB

a. Building _____

b. Floor _____ c. Area _____

5. EXPLAIN WHY CALLER WISHES TO INJURE OR KILL INNOCENT PERSONS

3. DID CALLER INDICATE KNOWLEDGE OF THE FACILITY?

☐ NO ☐ YES (Explain) _____

SECTION III — DESCRIPTION OF CALLER'S VOICE

☐ MALE ☐ FEMALE
☐ YOUNG ☐ OLD ☐ MIDDLE-AGED
☐ CALM ☐ NERVOUS ☐ REFINED ☐ ROUGH
☐ ACCENT ☐ SPEECH IMPEDIMENT

(Describe) _____

DO YOU RECOGNIZE VOICE?

☐ NO ☐ YES (Whose voice is it?) _____

SECTION IV — BACKGROUND NOISE

☐ TRAFFIC ☐ HORNS ☐ WHISTLES
☐ MUSIC ☐ BELLS ☐ AIRCRAFTS
☐ TAPE RECORDER NERVOUS ☐ MACHINERY

☐ RUNNING MOTOR (Type) _____
☐ OTHER _____

SECTION V — TELEPHONE LINE DATA

1. LINE ON WHICH CALL WAS RECEIVED ☐ LISTED NUMBER? ☐ UNLISTED NUMBER?

2. IS THIS A NIGHT NUMBER? ☐ YES *(Whose number?)* _____

3. HAS A BOMB THREAT CALL BEEN PREVIOUSLY RECEIVED ON THIS NUMBER?

☐ NO ☐ YES (Explain) _____

SECTION VI — REPORTING OF THREAT
Caution: DO NOT TALK TO OTHERS about incident.)

1a. NAME OF PERSON RECEIVING CALL

b. DIVISION AND TELEPHONE NUMBER

c. TIME AND DATE CALL RECEIVED

2. REPORT THREAT TO:
a. FEDERAL PROTECTIVE SERVICE DIVISION
b. DESIGNATED OFFICIAL
c. BUILDINGS MANAGER

Building Information Sheet

Building name _____

Building number _____

Address _____

_____

Year building completed _____

Type of construction _____

_____

Number of floors _____

Mezzanine(s) _____

_____

Basement(s) _____

_____

Gross floor areas _____ square feet

Net assignable floor area _____ square feet

Government occupied floors _____

_____

Other Tenants _____

_____

Fire alarm system and signals _____

_____

Automatic sprinkler system _____

Voice communications systems _____

Occupant Information Sheet

Begin with the lowest floor and work upward. Because agencies move, this sheet must be reviewed and updated acccordingly.

Primary occupant agency _____

Number of Federal occupants _____

Number of other occupants _____

Total occupancy _____

_____

_____

Floor	Occupant	Type of Occupancy	Contact phone number	Uses or stores hazardous materials, other special considerations

FIGURE A3-41.
OCCUPANT EMERGENCY PLAN—SAMPLE FORMAT

Command Center Team

(Update as necessary and check quarterly)

Building _____

Address _____

_____

Designated Official:

_____

Title

_____

Name of incumbent

_____

Telephone: Office Home

Occupant Emergency Coordinator:

_____

Title

_____

Telephone: Office Home

Floor Team Coordinator:

_____

Title

_____

Name of incumbent

_____

Telephone: Office Home

Floor Team—Floor _____

Complete one sheet per floor. Modify the sheet to correspond to your building's unique layout. In particular, appoint as many area and stairwell monitors as your building requires.

Floor Monitor _____
Title _____
Telephone _____
Skills _____

Area _____ Monitor _____
Title _____
Telephone _____
Skills _____

Area _____
Title _____ Monitor _____
Telephone _____
Skills _____

Stairwell _____ Monitor _____
Title _____
Telephone _____
Skills _____

Stairwell _____ Monitor _____
Title _____
Telephone _____
Skills _____

Monitors for the Handicapped

_____	_____
Monitor	Telephone
_____	_____
Handicapped person/handicap	Telephone
_____	_____
Monitor	Telephone
_____	_____
Handicapped person/handicap	Telephone

Evacuation Information

Person Authorized To Order Evacuation

Designated Official _____

Occupant Emergency Coordinator _____

Federal Protective Service Official _____

Building Manager _____

Fire Department Official in Charge _____

Evacuation Signals

Fire: Describe method of notification for complete or partial evacuation.

_____

_____

_____

_____

Explosion or Gas Leak: Describe method of notification for complete or partial evacuation.

_____

_____

_____

_____

Suspicious Object: Describe method of notification for complete or partial evacuation.

_____

_____

_____

_____

Evacuation/Bomb Search Chart

Building _____ Date _____

Floor/Area	TIME		Remarks
	Evacuated	Searched	

NOTE: This chart provides a useful tool for reviewing the effectiveness of an evacuation and/or search. Remarks may include who searched the floor or area, where persons were relocated, and any unusual circumstances.

Management Regulations

Part 101-20. Management of Buildings and Grounds
(Only relevant parts are included)

101-20.003. Definitions

(g) The "Designated Official" is the highest ranking official of the primary occupant agency of a Federal facility; or, alternatively, a designee selected by mutual agreement of occupant agency officials.

(i) The term "emergency" includes bombings and bomb threats, civil disturbances, fires, explosions, electrical failures, loss of water pressure, chemical and gas leaks, medical emergencies, hurricanes, tornadoes, floods, and earthquakes. The term does not apply to civil defense matters such as potential or actual enemy attacks. Note: Civil defense emergencies are addressed by the Federal Emergency Management Agency.

(v) "Occupant Emergency Organization" means the emergency response organization comprised of employees of Federal agencies designated to perform the requirements established by the Occupant Emergency Plan.

(w) "Occupant Emergency Plan" means procedures developed to protect life and property in a specific Federally-occupied space under stipulated emergency conditions.

(x) "Occupant Emergency Program" means a short-term emergency response program. It establishes procedures for safeguarding lives and property during emergencies in particular facilities.

101-20.103. Physical protection and building security

101-20.103-1. Standard protection

For properties under its custody and control, GSA will provide standard protection services by:

(g) Coordinating a comprehensive Occupant Emergency Program.

101-20.103-4. Occupant Emergency Program

(a) The Designated Official (as defined in 101.-20.003(g)) is responsible for developing, implementing, and maintaining an Occupant Emergency Plan (as defined in 101-20.003(w)). The Designated Official's responsibilities include establishing, staffing, and training an Occupant Emergency Organization with agency employees. GSA shall assist in the establishment and maintenance of such plans and organizations.

(b) All occupant agencies of a facility shall fully cooperate with the Designated Official in the implementation of the emergency plans and the staffing of the emergency organization.

(c) GSA shall provide emergency program policy guidance, shall review plans and organizations annually, shall assist in training of personnel, and shall otherwise ensure proper administration of Occupant Emergency Programs (as defined in 101-20.003(x)). In leased space GSA will solicit the assistance of the lessor in the establishment and implementation of plans.

(d) In accordance with established criteria, GSA shall assist the Occupant Emergency Organization (as defined in 101-20.003(v)) by providing technical personnel qualified in the operation of utility systems and protective equipment.

101-20.103-5. Initiating action under Occupant Emergency Programs

(a) The decision to activate the Occupant Emergency Organization shall be made by the Designated Officials, or by the designated alternate official. Decisions to activate shall be based upon the best available information, including an understanding of local tensions, the sensitivity of target agency(ies), and previous experience with similar situations. Advice shall be solicited, when possible, from the GSA buildings manager, from the appropriate Federal Protective Service Official, and from Federal, State, and local law enforcement agencies.

(b) When there is immediate danger to persons or property, such as fire, explosion, or the discovery of an explosive device (not including a bomb threat), occupants shall be evacuated or relocated in accordance with the plan without consultation. This shall be accomplished by sounding the fire alarm system or by other appropriate means.

(c) When there is advance notice of an emergency, the Designated Official shall initiate appropriate action according to the plan.

(d) After normal duty hours, the senior Federal Official present shall represent the Designated Official or his/her alternates and shall initiate action to cope with emergencies in accordance with the plans.

Occupant Emergency Plan Check List

If you can't check any of the following questions, your Occupant/Emergency Plan needs strengthening. Contact your building manager and/or the GSA Physical Security and Law Enforcement Office nearest you if you need help.

- ☐ Did an advisory committee of appropriate officials (Building Manager, Federal Protective Service, etc.) assist in developing the plan? Is this committee still available for consultation?
- ☐ Has an emergency organization been established, preferably following existing lines of authority?
- ☐ Are emergency organization members designated by position rather than by person?
- ☐ Do organization members know their own responsibilities as well as who has decisionmaking authority in any given situation?
- ☐ Has a procedure been established to notify organization members?
- ☐ Are emergency procedures easy to implement rapidly?
- ☐ Has a Command Center location been established?
- ☐ Are communications at the Command Center adequate?
- ☐ Do emergency organization members know under what circumstances they are to report to the Command Center?
- ☐ Are employees who do not have assigned duties excluded from the Command Center?
- ☐ Are emergency telephone numbers posted in the Command Center and throughout the building? Published in the telephone book?
- ☐ Are procedures established for handling serious illness, injury, or mechanical entrapment?
- ☐ Do organization members know what medical resources are available and how to reach them?
- ☐ Have all occupants been told how to get first aid/CPR fast?
- ☐ Do occupants know what to do if an emergency is announced?
- ☐ Are evacuation procedures established and familiar to all employees?
- ☐ Have special procedures been established for evacuation of the handicapped?
- ☐ Are fire-reporting procedures established and familiar to all employees?
- ☐ Have firefighting plans been developed which coordinate internal and external resources?
- ☐ Do occupants know to whom they should report an unlawful act? Any other emergency incident?
- ☐ Do employees know what procedures to follow if they receive a telephone bomb threat?
- ☐ Are bomb search responsibilities and techniques specified in the plan?
- ☐ Are procedures established for reporting the progress of a search, evacuation, etc.?
- ☐ Have procedures been established for bomb disposal?
- ☐ Have emergency shutdown procedures been developed?
- ☐ Have plans been made for capture and control of elevators?
- ☐ Have arrangements been made for emergency repair or restoration of services?
- ☐ Have drills and training been adequate to ensure a workable emergency plan?
- ☐ In leased space, is the responsibility of the owner/lessor clearly defined? If contract guards are used, have their authority and responsibilities been defined?
- ☐ Are floor plans and occupant information readily available for use by police, fire, bomb search squads, and other emergency personnel?
- ☐ Has a hazard communication program been implemented in accordance with 29CFR 1910.1200?
- ☐ Has an inventory been compiled of all hazardous materials used in individual workplaces and stored anywhere in the building?
- ☐ Are emergency telephone numbers displayed and/or published where they are readily available? Are they reviewed and updated frequently?

GSA Law Enforcement Offices

Central Office
Office of Physical Security and Law Enforcement (PS)
General Services Administration
18th and F Sts., NW.
Room 2314
Washington, DC 20405

National Capital Region
Washington, DC, and nearby Maryland and Virginia
Federal Protection Division (WPS)
Southeast Federal Center
3rd and M Streets, SE.
Building, 159E, Second Floor
Room 211
Washington, DC 20407

Region 2
New York, New Jersey, Puerto Rico, Virgin Islands
Law Enforcement Branch (2PML)
26 Federal Plaza, Room 17-130
New York, NY 10278

Maine, Vermont, New Hampshire, Massachusetts, Rhode Island, Connecticut
Law Enforcement District (2PML-XL)
Tip O'Neill Building
10 Causeway Street, Room 108
Boston, MA 22222

Region 3
Pennsylvania, Delaware, Maryland Virginia, West Virginia
Law Enforcement Branch (3PML)
Roberty N.C. Nix Federal Building and U.S. Post Office
9th and Market Sts. Room 3345
Philadelphia, PA 19107

Region 4
North Carolina, South Carolina, Georgia, Tennessee, Alabama, Mississippi, Florida, Kentucky
Law Enforcement Branch (4PML)
Summit Building
401 West Peachtree, Suite 2500
Atlanta, GA 30365

Region 5
Ohio, Michigan, Wisconsin, Indiana, Illinois, Minnesota
Federal Protection Division (5PS)
230 South Dearborn Street
Room 3540
Chicago, IL 60604

Region 6
Kansas, Misouri, Iowa, Nebraska
Law Enforcement Branch, (6PML)
1500 East Bannister Road
Room 2137
Kansas City, MO 64131

Region 7
Texas, Louisiana, Arkansas, Oklahoma, New Mexico
Law Enforcement Branch (7PML)
819 Taylor Street, Room 14A14)
Fort Worth, TX 76102

Colorado, Utah, Wyoming, Montana, North Dakota, South Dakota
Law Enforcement District (7PXML)
Denver Federal Center, Building 1
Denver, CO 80225

Region 9
California, Arizona, Nevada, Hawaii, Guam, Northern Mariana Islands
Law Enforcement Branch (9PML)
525 Market Street, 30th Floor
San Francisco, CA 94105

Washington, Oregon, Idaho, Alaska
Law Enforcement District (9PX-3L)
916 Second Ave., Room 2610
Seattle, WA 98174

APPENDIX 4. FAA STAFFED FACILITY TYPES

1. **FAA STAFFED FACILITY TYPES.** The following is a list of staffed facility types.

FIGURE 4-1. FAA STAFFED FACILITY TYPES

ACO	Aircraft Certification Office
ADO	Airports District Office
AEG	Aircraft Evaluation Group
AFO	Airports Field Office
AFS	Airway Facilities Sector
AFSFO	Airway Facilities Sector Field Office
AFSS	Automated Flight Service Station
AIFSS	Automated International Flight Service Station
AOM	Area Operations Manager
ARSR	Air Route Surveillance Radar
ARSR/JSS	Air Route Surveillance Radar/ Joint Surveillance Site
ARTCC	Air Route Traffic Control Center
ASR	Airport Surveillance Radar
ATCSCC	Air Traffic Control System Command Center
ATCT	Airport Traffic Control Tower
ATLO	Air Traffic Liaison Officer
ATREP	Air Traffic Representative
CASFO	Civil Aviation Security Field Office
CASFU	Civil Aviation Security Field Unit
CASIFO	Civil Aviation Security International Field Office
CASLO	Civil Aviation Security Liaison Officer
CCC	Child Care Center
CERAP	Center Radar Approach Control
CMFO	Certificate Management Field Office
CMO	Certificate Management Office
DISU	Drug Interdiction Support Unit
FAA REP	FAA Representative
FEU	F&E Field Unit
FIAO	Flight Inspection Area Office
FIFO	Flight Inspection Field Office
FIO	Flight Inspection Office
FISO	Flight Inspection Satellite Office
FMP	Field Maintenance Party

FPO	Flight Procedures Office
FSDO	Flight Standards District Office
FSDPS	Flight Service Data Processing Systems
FSFO	Flight Standards Field Office
FSIDO	Flight Standards International District Office
FSM	Federal Security Manager
FSS	Flight Service Station
IFO	International Field Office
IFSS	International Flight Service Station
IPTO	Integrated Product Team Office
LGFO	Logistics Field Office
MFO	Medical Field Office
MIDO	Manufacturing Inspection District Office
MISO	Manufacturing Inspection Satellite Office
NAVLO	Navy Liaison Officer
NEOF	National Emergency Operation Facility
NNCC	National Network Control Center
OTFO	Operations Technical Field Office
RAPCON	Radar Approach Control
RATCF	Radar Air Traffic Control Center
SMO	Systems Management Office
SSC	Systems Support Center
SSU	Systems Support Unit
TRACON	Terminal Radar Approach Control

APPENDIX 5. FAA FACILITY SECURITY LEVEL DESIGNATION

1. **PURPOSE.** This appendix establishes facility security levels and frequency requirements for the FAA Facility Security Management Program. The security levels established by this order are intended solely for security purposes and do not necessarily conform to any other category, operating level, or other form of facility designations or description used by another FAA Line of Business (LOB).

2. **DEFINITION.** FAA FACILITY. An FAA facility, for the purpose of this order, is defined as any FAA owned, leased, or staffed building, structure, warehouse, appendage, storage, and utilities, when related by function and location for an operating entity owned, operated, or controlled by the FAA.

3. **FACILITY SECURITY LEVELS FOR STAFFED AND UNSTAFFED FACILITIES.** Security level designations shall be assigned to all FAA facilities for the purpose of determining the required protective measures for each facility and to conform to a security assessment and inspection schedule that will evaluate the facility's security posture on an annual, biennual, triennial, or as-requested basis. In addition to assigning security levels to specific facility types, Table A5.1, FAA Facility Security Levels shall serve as a guide to assist Servicing Security Element (SSE) in determining the appropriate security level designations for new facilities. The facility type descriptions found in table A5.1 should be used to determine the appropriate security level designations for facilities not specifically listed. A higher security level designation may be assigned to a facility, although not meeting the facility description in table A5.1, when the facility has been determined by the respective line of business, in coordination with the SSE, as critical to the National Airspace System (NAS). FAA facilities listed is Table A5.1, and others meeting similar characteristics, shall be assigned one of the following security category designations:

a. Security Level 4 (SL4). Security Level 4 designated facilities will usually have more than 450 employees, more than 150,000 square feet of space, house highly sensitive records, and may have a high volume of public contact.

b. Security Level 3 (SL3). Security Level 3 facilities will usually have between 151 and 450 employees and have between 80, 000 and 150, 000 square feet of space. These facilities are considered mission critical and total destruction, loss, or major damage may have a very serious or catastrophic impact on the NAS. These facilities may contain Classified or COMSEC equipment and material.

c. Security Level 2 (SL2). Security Level 2 facilities will usually have between 11 and 150 employees, 2,500 to 80,000 square feet of space, and a moderate volume of public contact. These facilities are considered essential to the FAA and NAS and total destruction, loss, or major damage may have a moderate to serious impact on the agency's mission accomplishment.

d. Security Level 1 (SL1). Security Level 1 facilities will usually have 10 or fewer employees, less that 2,500 square feet of space, and only a small amount of public contact or no public contact at all. Total destruction, loss, or major damage to this type of facility would not have a significantly adverse impact on the NAS or the agency in accomplishing the FAA mission.

e. Security Level 1A (SL1A). Generally, Security Level 1A facilities includes all FAA unstaffed facilities which do not have any FAA employees assigned or reporting as a post of duty.

Exceptions to this definition are those unstaffed facilities where classified documents, materials, COMSEC equipment, and equipment or systems critical to the NAS may be stored.

FIGURE A5-1. FAA FACILITY SECURITY LEVELS

Facility Security Level	FAA Facility Types	Evaluation Frequency	Facility Description
4	• FAA National Headquarters Office • Regional Office Buildings • Mike Monroney Aeronautical Center (MMAC) • FAA Technical Center	Annual	These facilities have over 450 employees during any single established work period; likely has more than 150K square feet of space; and may have high volume public contact. These facilities are considered mission critical and total destruction, loss, or major damage may have a catastrophic impact on the National Air Space (NAS).
3	• Air Traffic Control System Command Center • (ATCSCC) • Air Route Traffic Control Center (ARTCC) • Airport Traffic Control Towers (Level 5) • Center Radar Approach Control (CERAP) • Combined Terminal Radar Approach Control • (TRACON)	Annual	A facility with 151 – 450 employees during any single established work period; likely has between 80K and 150K square feet of space; and may have a moderate to high volume of public contact. These facilities may be collocated with high risk law enforcement and intelligence agencies, courts, judicial offices, or other highly sensitive government offices. These facilities are considered mission critical and total destruction, loss, or major damage may have a very serious or catastrophic impact on the NAS.
2	• Airport Traffic Control Towers (Level 3-4) • Air Route Surveillance Radar (ARSR) • ARSR/Joint Surveillance Sites (ARSR/JSS) • Area Operations Manager (AOM) • Automated Flight Service Station (AFSS) • National Network Communication Center (NNCC) • Certificate Management Office (CMO) • Civil Aviation Security Field Office (CASFO) • Flight Standards District Office (FSDO) • Radar Approach Control (RAPCON) • Systems Management Office (SMO)	Biannual	A facility with 11 – 150 employees during any single established work period; likely has between 2.5 and 80K square feet of space; and may have a moderate volume of public contact. These facilities are considered essential to the FAA and NAS and total destruction, loss, or major damage may have a moderate to serious impact on the agency's mission accomplishment. **Note: ARSR/JSS facilities will be inspected annually and required protective measures shall in accordance with the Physical Security Design Criteria for the FAA/USAF ARSR-4 Program memo dated July 19, 1989.** **Note: Due to the uniqueness and importance to the NAS, NNCC's that are collocated with ARTCCs shall be protected at the same level as the ARTCC.**

FIGURE A5-1. FAA FACILITY SECURITY LEVELS (cont.)

Facility Security Level	FAA Facility Types	Evaluation Frequency	Facility Description
1	• Airports District Office (ADO) • Airport Traffic Control Towers (ATCT) • (Level 1-2) and FCTs • Air Traffic Evaluations (ATH) • Civil Aviation Security Field Unit (CASFU) • Flight Inspection Office (FIO) • Flight Service Station (FSS) • Flight Inspection Field Office (FIFO) • International Field Office (IFO) • International Flight Service Station (IFSS) • Staffed Airport Surveillance Radar (ASR) • Systems Support Center (SSC) • Systems Support Unit (SSU • Manufacturing Inspections District Office (MIDO) • Medical Field Office (MFO)	Triennial	This type of facility has 10 or fewer employees; likely has 2.5K square feet, or less, of office space; and a low volume of public contact or contact with only a small segment of the population. These facilities are considered essential to the agency's mission accomplishment. Total destruction, loss, or major damage to this type of facility would not have a significantly adverse impact on the NAS or the agency in accomplishing the FAA mission. ATCT participating in the FCT program with or without FAA employees reporting for duty at these locations will all be designated Security Level 1 facilities.
1A	• Unstaffed FAA facilities [e.g., Remote Transmitter Receiver (RTR), Remote Communications Link (RCL), Low Level Wind Shear Alert System (LLWAS), Outer Marker (OM), Middle Marker (MM), Radio Communications Link Repeater (RCLR), Localizer (LOC), Airport Surveillance Radar (ASR), VHF Omni-Directional Range, etc.	As required	Unstaffed equipment facilities.

Note 1: In situations where two or more organizations meeting different security level definitions are collocated in a single facility, the highest security level and evaluation frequency will be applied to all organizations.

Note 2: For facilities which store classified information or communications security (COMSEC) equipment, evaluation requirements and frequency will be in accordance with applicable FAA orders governing classified or COMSEC equipment.

Note 3: Facilities determined to be critical to the NAS may be designated a higher security level than required by figure A5-1.

Note 4: The facilities that are not identified in the tables above, and notes 1-3 are not applicable, the numbers of employees as identified in the facility description will determine the facility security level.

APPENDIX 6. PERIMETER AND ENTRY CONTROLS

1. **OBJECTIVE.** To establish exterior physical security protective measures for FAA facility perimeter controls for new and existing facilities.

SECTION 1. PERIMETER CONTROLS

2. **PERIMETER CONTROLS.** Perimeter protection is the first line of defense in providing physical security for a facility. Protecting the outer perimeter of a facility may be accomplished by installing fences or other physical barriers, exterior lighting, closed circuit television (CCTV) cameras, perimeter intrusion detection systems (PIDS), vehicular controls to include parking, site signage, landscaping, or by a security guard force. Often a combination of two or more of these controls will be the most effective.

3. **SITE PERIMETER BARRIERS.** In addition to defining the physical limits of a facility and controlling access, a perimeter barrier also:

a. Reduces or eliminates the possibility of accidental entry.

b. Deters unauthorized entry.

c. Aids the security guard force in controlling access and facilitates their effective utilization.

d. Provides control capability for persons and vehicles through designated entrances.

e. Can be used as a base for mounting a perimeter intrusion detection system (PIDS) providing an interactive barrier supporting the perimeter fence.

4. **FAA STANDARD SECURITY FENCE.** Critical operational FAA facilities will normally have requirements for an FAA standard security fence as a perimeter barrier. Construction of an FAA standard security fence and gates shall be accomplished in compliance with specifications contained in this appendix. While there is a need for consideration of fencing not meeting FAA standards, such as vinyl coated fabric with knuckled selvage at child care centers and livestock barriers at leased sites, perimeter fence specifications that deviate from requirements outlined in this section must be coordinated and approved by ACO-400.

a. Siting. Whenever locations permit, perimeter fencing shall be located not less than 300 feet from the object of protection.

b. Clear zone requirement. Perimeter fencing shall be constructed so that an unobstructed area or clear zone is maintained on both sides of the barrier. Where CCTV systems are employed for visual assessment purposes, clear zones shall be of sufficient width to present an unobstructed view of the perimeter barrier. Clear zone requirements shall be 20 feet on both sides of the perimeter fence.

c. Grounding requirement. Fencing shall be grounded in accordance with requirements outlined in FAA-STD-019.

d. Fabric. Fences, including gate structures, shall be of 9-gauge or heavier chain link fabric. Fabric shall be aluminum or zinc-coated steel wire chain link with meshes openings not larger than 2 inches on a side (FAA specification FAA-E-2065). The top and bottom edges of the fence fabric shall be twisted or barbed.

(1) Fabric ties. Fence fabric shall be attached to the exterior side of line posts using not less than 9-gauge steel ties. If the ties are coated or plated, the coating or plating will be electrolytically compatible with the fence fabric to inhibit corrosion. Ties will be spaced not more than 14 inches apart.

(2) Height. The standard height of an FAA security fence shall be 8 feet. This includes a fabric height of 7 feet plus a top guard extension of 1 foot. The fence fabric must be within 2 inches of packed ground and will be anchored in such a manner as to preclude the fence fabric being lifted more than 4 inches from the ground.

(3) Stretcher bars. Fence fabric shall be attached to terminal posts with stretcher bars 0.25 inches by 0.75 inches, which engage each fabric link. The stretcher bars shall be held to the fence post with clamps in such a way as to hold the fabric taut. The clamps for the stretcher bars shall be placed within 4 inches of the top and bottom rail, and shall be spaced not more than 14 inches apart.

e. Top Guard. A top guard is required on all FAA standard chain link security fences and gates. The top guard shall:

(1) Face outward and upward at an angle of 45 degrees from the horizontal.

(2) Have support arms that are constructed of 12-gauge pressed steel, permanently affixed to the top of the fence posts by riveting or other approved method, to increase the overall height of the fence by a minimum of 1 foot.

(3) Have support arms that must be so constructed and secured to the fence post that they will withstand an actual test pull down of a vertical load of 250 pounds without sagging or bending.

(4) Have 3 strands of 12-gauge barbed wire with 4-point barbs spaced 4 inches apart and stretched taut between the support arms.

(5) Have the top strand of barbed wire 12 inches above and parallel to the fence line, with the remaining 2 strands spaced uniformly between the top of the fence fabric and the top strand.

f. Reinforcement. Taut reinforcing wires a minimum of 9-gauge shall be installed and inter-woven with or affixed with 12-gauge fabric ties spaced uniformly between the top and bottom of the fence fabric.

g. Fencing Posts And Hardware. All fence posts, supports, and hardware for FAA standard security fences shall meet the requirements of Federal Specification RR+F-191J/GEN of July 1981.

(1) All fastening and hinge hardware shall be secured against attempts at unauthorized removal by methods approved by the SSE.

(2) All posts and structural supports shall be located on the interior of the fence. Posts shall be spaced not more than 9 feet apart and shall be embedded in bell shaped concrete footings to a depth of at least 2 feet to prevent shifting or sagging. Fence posts at ARSR-4 JSS facilities shall be spaced at not more than 6 feet apart due to agreements between the FAA and the U.S.A.F.

h. Culverts and Troughs. Where the perimeter fence traverses culverts, troughs, ditches, or other openings greater than 96 square inches in area, the opening shall be protected by an extension of the fence construction. This extension may consist of iron grills, barrier structures, or other barriers of a design approved by the SSE for the purpose of preventing unauthorized access.

(1) Bars and grills shall be installed in such a way that they do not impede required drainage.

(2) Hinged security grills used with an approved high security hasp, shackle, and padlock, which can be opened when necessary, is often a workable solution to securing drainage structures.

i. Gates. Construction. Security fence gates shall be constructed of a galvanized tubular steel framework. The following requirements apply:

(1) The steel used in the framework shall have a minimum outside diameter of 2 inches and a weight per linear foot of not less than 2.75 pounds.

(2) Framework shall be trussed to limit sagging and provide additional strength.

(3) Large gates shall have horizontal and vertical support members of the same type and size as the outside network.

(4) Fabric used for gate construction shall be of the same type and quality specified for the remainder of the fence and shall be attached in the same manner.

(5) Hardware used on swing gates shall have the securing bolts placed on the inside and secured or modified in a manner approved by the SSE to deter their unauthorized removal.

(6) Bolts used on sliding gates, which hold the trolley wheels in place, shall be secured and/or modified to make unauthorized removal difficult.

(7) Ground clearance. The space between the bottom edge of the gate and the pavement or firm ground should not exceed 4 inches. Where the gate is situated over a sharply graded street as is often found with vehicular gates, excessive gaps can occur beneath the gate. In addressing this problem, the SSE will provide the facility manager with appropriate guidance for meeting the security standard. Some approaches include the use of cantilevered or overhead gate structures which are recessed into subsurface troughs or provision for an extension on the bottom edge of swinging gates which can be lowered into a slotted channel extending beneath ground level when the gate is closed.

j. Gate Locks. The locking mechanism for a gate shall be installed on the inside. The following requirements apply:

(1) The lock shall be protected with steel shields to prevent tampering with the mechanism from the outside.

(2) Eyebolts can be welded to the fence frame and gateposts when necessary to permit secure locking.

(3) Use of a chain and padlock shall be avoided whenever possible, because the chain permits an excessive distance between single gates and the gateposts, and between the frame of double gates. In those instances where it is determined that a chain and padlock is the only feasible solution to securing a gate structure, the facility manager shall consult with the SSE to determine the specific installation and control requirements.

k. Gate Entrances. The number of perimeter gates which are designated for active use, shall be kept to the absolute minimum required for operations. This means that provisions shall be made for sufficient entrances to accommodate the peak flow of both pedestrian and vehicular traffic, as well as provisions for adequate lighting for efficient inspection.

l. Unattended Gates. Gates that are not attended shall be securely locked at all times. Protective lighting shall be provided to deter attempts at tampering during the hours of darkness. PIDS, CCTV, and other protective measures shall be considered when determined to be necessary based on the facility evaluation to meet safeguarding requirements.

m. SemiActive Gates. Gates which are used occasionally, shall be protected in the same manner prescribed for unattended gates during those periods when the gates are not under the direct visual observation and control of a security guard.

n. Special Requirements.

(1) Gates over 6 feet in height shall be secured so that the gate cannot be pried a sufficient distance to allow unauthorized entry.

(2) Vehicular gates. Vehicular gates shall be set well back from the public highway or access road in order that temporary delays caused by identification control checks at the gate will not cause undue traffic congestion. Sufficient space shall be provided at the gate to allow for spot checks, inspections, searches, and temporary parking of vehicles without impeding traffic flow.

(3) PIDS. Usually gates are protected by the use of locks and intermittent patrol checks or by fixed posts. The use of PIDS devices at gate entrances has to be justified on the basis of identified need. If the gate is used only intermittently, or if additional protection is desired for the gate portion of the facility perimeter fence line, the use of PIDS may be considered either separately or in combination with other devices. Among the various devices that can be employed for controlling access at gate entrances are electronic card access devices and CCTV. These additional requirements will be determined based on the facility evaluation.

(4) CCTV either in the surveillance mode or in the motion-sensing mode of operation can be very useful in physical security operations and is frequently used within the Federal Government to serve as an admittance verification and control or to verify an alarm condition in support of other sensors. These functions are served by placing CCTV cameras in critical locations with direct visual monitoring capability from a remote vantage point.

(a) CCTV may be used on gates that are not attended continuously. This system consists of a CCTV camera, monitor, and associated electrical and communications circuitry. The camera is remotely controlled by the monitoring personnel at designated locations. CCTV on gates shall include the use of a two-way communications system between the monitor panel at a designated location and the protected gate access point. With this capability, the person at the designated monitoring location can communicate with the individual seeking entry and, after verifying his or her authority to enter, can remotely release the gate lock.

(b) Controls for CCTV shall be enclosed in metal housing, have tamper alarms, and properly secured to prevent any tampering by unauthorized personnel.

5. CLEAR ZONE. The FAA standard security fence shall be constructed so that an unobstructed area of clear zone is maintained on both sides of the barrier. For design and engineering purposes, the interior and exterior clear zones should be a minimum of 20 feet.

a. A fence that is not protected with PIDS and CCTV is likely to be very vulnerable to unauthorized access if it is not under constant surveillance. The purpose of the clear zone is to make it more difficult for potential intruders to conceal themselves from observation.

b. The clear zone shall be free of objects or features which would offer concealment or which could facilitate unauthorized access.

6. WHEN THE CLEAR ZONE REQUIREMENT CANNOT BE MET. When for operational, environmental, or other reasons it is not practical to establish the required clear zone at a facility, the SSE shall coordinate with the facility manager to develop viable compensatory measures. The SSE will evaluate the risk and vulnerability associated with the fence and additional protective measures will be required. These measures may include increasing the height of portions of the fence, providing increased lighting in the affected area, installing CCTV surveillance cameras monitored from another location, installing PIDS, and increasing guard patrols.

SECTION 2. PROTECTIVE LIGHTING

7. OBJECTIVE. The objectives of protective lighting are to:

a. Discourage or deter attempts at entry by intruders during hours of darkness.

b. Increase the probability of detection at attempts at intrusion.

c. Permit the identification and inspection of persons and vehicles entering or departing the facility premises through designated control points.

8. GENERAL. Protective lighting consists of perimeter, parking, entry, and facility lighting. Protective lighting should not be used as a psychological deterrent only. It should be used on a perimeter fence only where the fence line is under continuous or periodic observation. Where protective lighting is required it shall be of the continuous type. (For types of lighting see section 5.) Protective lighting systems shall be connected to the emergency power system to ensure they remain operational during periods when commercial power is interrupted.

a. Perimeter lighting. Where perimeter lighting is required, the lighting units for a perimeter fence shall be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area on both the inside and outside of the fence. Perimeter lighting shall be continuous and on both sides of the perimeter fence and shall be sufficient to support CCTV and other surveillance equipment where required. The distance between each perimeter light pole and the perimeter fence is termed "standoff." For design purposes, the standoff will not be less than 20 feet. The standoff area shall be as flat as possible and kept free of vegetation. Generally, the light band should illuminate the fence barrier and extend as deeply as possible into the approach area. The distance between poles used to mount luminaries along the perimeter shall not exceed four times the mounting height. Perimeter lighting mounting poles shall be located inside the perimeter fence and meet standoff requirements specified in the paragraph above.

b. Parking Lot Areas. Parking lots shall be provided with uniform illumination. In addition to the security hazard of providing hiding places, parking lots are vulnerable to pilferers and can pose a risk to employees from the standpoint of vulnerability to physical attack. (See paragraph 26 for more details.)

c. Entry Point Lighting. Pedestrian and vehicle entrances shall be provided with lighting in such a way that they that the lighting is sufficient for recognition of persons and examination of credentials.

(1) Pedestrian and vehicle entrances that are semiactive shall have the same degree of continuous lighting as the remainder of the areas being lit.

(2) Security gate houses at entrance points shall have a reduced level of interior illumination enabling guards to see better, increase their night vision adaptability, and avoid making them a target.

SECTION 3. OTHER PERIMETER CONTROLS

9. FAA WARNING SIGNS. Warning signs shall be provided on perimeter fences and all sides of ATS facilities. There shall also be on site directional, parking, towing, and signs identifying the facility as being monitored by CCTV if applicable. FAA Warning signs identifying facilities as important to air safety and warning against trespass or attempts to damage the facility shall be affixed to all FAA standard security fences and to FAA buildings and structures in accordance with the following requirements.

a. Fences. FAA warning signs shall be affixed to all FAA ATS facility's perimeter fencing at intervals of 50 feet. In areas where the use of a second language other than English is prevalent, bilingual warning signs shall be installed adjacent to the regular FAA warning sign.

b. Buildings. FAA buildings and structures involved in air traffic operations. Building and structure FAA warning signs shall be installed on the building or structure at logical avenues of approach. For irregular shaped and smaller buildings and structures, the signs shall be posted in such a way that they are plainly visible to anyone approaching the building or structure.

c. Procurement. FAA warning signs may be procured from the FAA Depot, Oklahoma City. The signs have been printed on two materials, metal and heavy paper card stock. The stock numbers are NSN 9099-00-056-9704 (metal) and NSN 9099-00-056-9703 (paper).

10. CONTROL OF FACILITY PARKING. Where required, access to government parking shall be limited to government vehicles, personnel, and authorized visitors. This can be accomplished by use of a trained guard force, parking lot barriers such as barrier arms, or at a minimum, designation and identification of authorized parking spaces. Visitor parking shall be clearly marked.

11. CONTROL OF ADJACENT PARKING. Where determined as required based on facility evaluation, areas adjacent to FAA facilities shall be controlled to reduce the potential for threats against FAA facilities and employee exposure to criminal activity.

12. TOWING SIGNAGE. Procedures for the towing of unauthorized vehicles at FAA facilities shall be established. Local towing companies may be utilized for this service. Where required, signage shall be posted in all parking areas warning of the risk of the towing of unauthorized vehicles.

13. VEHICULAR IDENTIFICATION SYSTEMS. Facilities required to implement a vehicular identification system must do so in accordance with FAA Order 1600.25.

14. CLOSED CIRCUIT TELEVISION WITH TIME LAPSE VIDEO RECORDING. CCTV is very useful in physical security operations and is frequently used to compliment an alarm system. The system consists of television cameras, monitors, and associated circuitry. Normal use of this system includes the use of a two-way communication system between the monitoring point and a facility entrance plus an electronically operated lock. The use of a CCTV system economizes on personnel requirements and provides security to the facility by allowing positive identification prior to facility admittance. Where required, CCTV shall be used for monitoring and recording security incidents in the following areas:

a. Personnel entrances, monitored exits, vehicular entrances, parking areas, garages, and loading docks.

b. CCTV systems should be designed for the purpose of viewing alarmed areas and assessing the need for a security response.

c. CCTV cameras shall be real-time with the capability for time lapse recording.

d. Exterior CCTV shall monitor uncontrolled alarmed doors, emergency exits, and the PIDS.

e. Perimeter CCTV systems shall be commercial off the shelf, that comply with FAA standards and specifications for surveillance and assessment systems.

f. Where CCTV surveillance is employed, signs warning of surveillance shall be posted so as to be visible to anyone approaching the camera's view.

SECTION 4. ENTRY CONTROLS

15. BUILDING CONTROLS. After perimeter safeguards have been established, the next concern relates to the exterior building controls. For FAA facilities that do not have a perimeter security fence, the exterior of the facility becomes the perimeter. In these instances, the building exterior serves as both the primary and secondary lines of security safeguards. This section establishes physical security criteria.

16. SHIPPING AND RECEIVING PROCEDURES. FAA facilities having a loading dock shall review current procedures to ensure deliveries are supervised and not left unattended. Facilities employing a guard force shall have guard force personnel telephonically notify facility management that a vehicle is enroute to the loading dock. Access and entry into the facility loading dock shall be controlled and where required observed by CCTV. All personnel who may receive or make shipments shall be aware of procedures employed by the facility to ensure the security of the loading dock area and all shipping and receiving procedures.

17. INTRUSION DETECTION SYSTEM WITH CENTRAL MONITORING CAPABILITY. Where required, intrusion detection systems shall be employed to detect attempts at unauthorized entry into a facility.

18. POSITIVE FACILITY ACCESS CONTROL. The number of active doors that can be used to gain access to an FAA facility or office shall be kept to the minimum necessary to support operations. Facilities shall not be configured with exterior doors placed for the purposes of convenience. All exterior doors to FAA facilities shall be locked at all times when not in immediate use. Doors identified as entrances shall be located in such a way that visitors must identify themselves to a receptionist, guard, or through CCTV monitoring.

a. PEEP HOLES. Peepholes serve as an easy and effective means of visual recognition system for smaller facilities.

b. INTERCOM. Intercoms serve as a communication tool that can be used in combination with the peephole. This is also effective at smaller facilities.

c. ENTRY CONTROL WITH CCTV AND DOOR STRIKES. CCTV cameras mounted at main entrance doors with strike releases strategically located throughout the facility are a means for allowing entry for smaller facilities when staffing levels may be at a minimum. They shall be used in conjunction with intercoms and allow the employees to view and communicate remotely with visitors before allowing access.

19. WINDOWS. Window openings, like doors, can be an inviting target for potential intruders. They also can serve as a means for removing agency property and documents from a facility. Windows, like doors, have an aesthetic value and when considering protective measures these concerns must be addressed. Fire and safety concerns must also be coordinated by the SSE when considering protective measures that would affect window openings.

a. Facility windows located on the first floor shall be secured on the inside. The mechanism used to secure the window may be a bolt, slide bar, or crossbar. Where the facility evaluation deems additional security measures are required, the SSE will coordinate with the facility manager on additional protective measures such as IDS.

b. Windows shall be of sturdy construction and properly set into substantial frames. The window frame must be securely fastened to the building so that it cannot be pried loose and the entire window removed. Outside window hinges shall be modified in a method approved by the SSE to prevent unauthorized removal.

c. Where glass makes up the exterior wall of a facility, the glass shall be sufficient strength to deter breakage. In addition, the interior side of the glass will be sensored to detect breakage and unauthorized exit.

d. As a design goal for new construction or major modifications to existing facilities, the installation of shatter resistant glass shall be used. These measures will be coordinated with the SSE during the design phase.

20. EXTERIOR DOORS. Exterior doors with the exception of main entrances shall be of substantial metal or solid wood construction. Exterior doors which provide direct access to Critical Areas shall be secured with FAA standard Best locks and cores (7-pin). Heavy-duty hardware shall be used throughout. Panic hardware will be installed on all exit doors and shall be alarmed to detect unauthorized entry attempts. Architectural conformity and concern for aesthetics often require that door structures be less substantial than desired. Main entrances employing glass and metal doors will be of solid construction and use tempered or safety glass.

a. Hinges shall be located on the inside of the door, concealed, or otherwise installed so as to be inaccessible from the exterior side when the door is closed.

b. If this is not possible, the hinge pins shall be installed so they cannot be removed by removing the screws. Hinge pins in exterior mounts shall be welded, flanged, or otherwise modified in a manner approved by the SSE to prevent their removal.

21. ROLLING OVERHEAD DOORS. Rolling overhead doors that are not controlled or locked by electric power shall be protected by slide bolts on the bottom bar. Chain-operated doors shall be provided with a cast iron keeper and pin for securing the hand chain. For crank operated doors, the protective measures taken must prevent unauthorized use of the door either by immobilizing the crank or locking the door to the frame with agency approved padlocks or both.

22. SOLID OVERHEAD, SWINGING, SLIDING, OR ACCORDION TYPE DOORS. This type of door shall be secured with a high security cylinder lock or a high security padlock, in conjunction with a metal slide bar, bolt, or deadbar on the inside.

23. METAL ACCORDION GRATE OR GRILL TYPE DOORS. This type of door shall have a secure metal guide track at the top and bottom and be provided with a high security cylinder lock or padlock which will provide the necessary protection.

24. MISCELLANEOUS OPENINGS AND KEY UTILITIES.

a. Manholes. Many FAA facilities have manholes which provide entrances into the buildings for service purposes. Others may provide access to utility tunnels containing pipes for heat, gas, water, telephone transmission conduits, cables, and other utilities.

(1) Manhole covers on FAA property must be secured if they provide access to an FAA building or to any communications or other utility lines servicing that building or operation.

(2) A case hardened chain and FAA approved high security padlock will be used to secure a manhole cover. The use of a heavy duty hinged steel deadbar secured with an FAA approved high security padlock and heavy duty hasp is another alternative method for security of manhole covers.

b. Accessible Steel Grates and Doors. Grates and doors on ground level are other potential access points into a facility. These types of openings often serve as service entrances, exterior elevator entrances, or they may simply provide light and air to the basement level of the building. If the mounting frame is properly secured, the grates or doors can be welded into place, or they can be secured with a case hardened chain and an FAA approved high security padlock.

c. Sewers and Storm Drains. These features shall be secured if the areas of the openings associated with them are larger than 96 square inches (0.06 square meters).

d. Rooftop Access Points. Rooftop structures can present readily available points of access to a potential intruder. An advantage of accessing a building from the roof is that an intruder can often work without the risk of detection once he or she has gained access to the roof area. Openings in elevator penthouses, roof top hatchways, and trap doors are sometimes omitted from a building's safeguarding plan because they are not often used.

(1) Rooftop access points shall be secured by FAA approved high security padlocks, locks, security bars, etc. Where deemed necessary, these openings should be alarmed to prevent unauthorized entry attempts.

(2) Skylights and similar structures shall be protected with steel bars or mesh. Such protection shall be installed inside the opening to make it more difficult to remove.

e. Transoms. Transoms may appear to be small, but they must not be overlooked as points of potential unauthorized access. A simple solution may be to seal the transom permanently. However, if this is not possible, each transom must be locked from the inside with a sturdy sliding bolt lock or other similar device, or be equipped with steel bars or grills installed on the inside.

f. Ventilating Shafts, Vents, or Ducts. Ventilating shafts, vents, and ducts represent possible points of unauthorized access into the facility. A ventilating shaft or duct may be large enough to permit a potential intruder access into the building from the exterior. Security openings of this type will require provision of effective man-barriers that will deter physical access while at the same time not interfere with the flow of air in the case of ventilating apertures. Normally, the use of steel bars set into a sturdy frame affixed to the duct or wall vent will provide the needed safeguard. Bars provide less impediment to air flow than security mesh or screens.

g. Key Utilities. Facilities will ensure that key utility areas are secure and that only authorized personnel can gain entry.

25. METAL DETECTION AND X-RAY SCREENING OF ALL MAIL AND PACKAGES. Visitors to FAA Security Level 3 and 4 facilities must pass through a metal detection device prior to entering the facility. Where required, all mail and packages shall be screened by x-ray immediately upon delivery to the facility. Personnel who are responsible for the screening shall be properly trained. They shall be able to identify suspicious packages and know the procedures for reporting such incidents.

Training shall be included as part of the procurement request for the x-ray equipment. Only persons certified as trained by the manufacturer will be allowed to operate X-ray screening equipment. Personnel to be trained shall be at the discretion of the facility manager.

26. ENTRY AND PARKING LOT LIGHTING. The cone of illumination from lighting units shall be directed downward and away from the structure or area being protected and away from security guards assigned to provide such protection. The lighting shall be so arranged as to create a minimum of shadows and a minimum of glare in the eyes of security guards. The objectives of protective lighting are to:

a. Discourage or deter attempts by intruders during hours of darkness.

b. Increase the probability of detection of attempts at intrusion.

c. Permit the identification and inspection of persons and vehicles entering or departing the facility premises through designated control points.

27. APPLICATION. Parking lot and entry lighting shall be in accordance with section 4 and shall be sufficient to allow personnel identification during the hours of darkness and extreme environmental conditions.

a. All pedestrian entrances to the facility shall be illuminated. They shall be provided with two or more lighting units installed in such a way that they provide adequate illumination for recognition of persons and examination of credentials.

b. Parking Lot Areas. Parking areas shall be provided with uniform illumination. In addition to the security hazard of providing hiding places, parking areas are vulnerable to pilferers and can pose a risk to employees from the standpoint of physical attack.

c. Security Guard Gate Houses. Gate houses at entrance points shall have a reduced level of interior illumination to enable the security guards to see better, increase their night vision adaptability, and avoid illuminating them as a target.

d. Emergency Power. Parking lot and entry lighting systems at FAA facilities shall be connected to the emergency power system to ensure they remain operational during periods, when commercial power is interrupted at critical facilities, and where emergency power systems are available.

SECTION 5. TYPES OF LIGHTING.

28. LIGHTING SYSTEMS. There are four general types of protective lighting systems. Making the determination as to which system is appropriate for a given application will depend upon the overall security environment and the requirements of the facility concerned.

29. CONTINUOUS LIGHTING. This is the most commonly used form of protective lighting systems and the type that is specified for FAA facilities. It consists of a series of fixed luminaries arranged to illuminate a given area on a continuous basis with overlapping cones of light during the hours of darkness. The two primary methods of employing continuous lighting are:

a. Glare projection. This type of lighting is useful where the glare of lights directed toward the exterior of the facility and into the eyes of a potential intruder is the desired effect. At FAA facilities, the lighting at gate entrance locations is an example of one application of this method. A vehicle approaching the gate during the hours of darkness is fully illuminated, but the guard station remains in the shadow of the light pattern.

b. Controlled lighting. This method is used most often at FAA locations where it is necessary to limit the width of the lighted strip outside the perimeter fence because of nearby residential areas, public thoroughfares, and other activity center. In controlled lighting, the width of the illuminated strip can be controlled and arranged as required. For instance, one possible configuration might be to have a wide band of illumination inside the fence and a much narrower band on the exterior of the fence. The design of the luminaries permits directing the light source to achieve these results. The angle of the luminaries is primarily downward with some angle adjustment to attain the desired bandwidth.

c. Surface lighting. Addresses those lighting systems that are used to provide required levels of illumination for critical areas and structures.

30. STANDBY LIGHTING. The arrangement of this system is similar to the continuous lighting array. The difference is that the luminaries are not continuously lighted during the hours of darkness but are activated manually or automatically when the security guard force or IDS detect suspicious activity.

31. MOVABLE LIGHTING. This type of lighting consists of manually operated movable light sources and luminaries, often searchlights, which may be lighted during the hours of darkness to cover specific areas as needed. Movable lights are normally used to supplement continuous or standby systems.

32. EMERGENCY LIGHTING. This system may duplicate the other three systems in whole or in part. Its use is normally limited to periods of main power failure or other emergencies. Security lighting at FAA facilities shall be connected to the emergency power systems. Emergency lighting depends on alternative power sources such as generators or batteries.

33. INCANDESCENT LAMPS. A median-efficient luminarie with a long life, it has good color rendition, has quick strike and restrike times, but is fragile and has a limited operating range in extreme temperature environments. These are common glass light bulbs in which the light is produced by the resistance of a filament to an electric current. Special purpose bulbs are manufactured with interior coating to reflect the light, with built-in lenses to direct or diffuse the light, or the naked bulb can be enclosed in a shade or luminaries fixture to accomplish the same results. It is recommended for climate

controlled interior applications where color CCTV is used, and where habitation or work is being performed.

a. Advantages: Instant start, good light control, good color retention, and lowest initial cost.

b. Disadvantages: High operating costs, short lamp life (500-2000 hours), 20 lumens per watt.

34. MERCURY VAPOR. These lamps emit a blue-green light caused by an electric current passing through a tube of conducting and luminous gas. They are more efficient than incandescent lamps of comparable wattage and are in widespread use for interior and exterior lighting, especially where people are working.

a. Advantages: Long lamp life, 50 lumens per watt, low operating costs compared to incandescent.

b. Disadvantages: Limited light control (beam spread or pattern), high initial cost, does not restart immediately after a power failure.

35. SODIUM VAPOR. Sodium vapor lamps are constructed on the same general principle as mercury vapor lamps but emit a golden yellow glow. High Pressure Sodium are the most cost efficient luminaries but have no color rendition. It has a wide range of operation in extreme temperature conditions, has a long strike and re-strike time, and is recommended for exterior applications where black-and-white CCTV is used. These lamps can be color corrected by using special lenses. Low Pressure Sodium is less efficient but long lived and durable with a long strike and restrike time. It has a amber-shifted color rendition and is not recommended for applications used with CCTV.

a. Advantages: Good light pattern control, long lamp life, and 103 lumens per watt.

b. Disadvantages: Higher initial cost. Not suitable on applications where process color rendition is critical, but some lamps are designed to be color-corrected.

36. METAL HALIDE. Metal Halide is a highly efficient luminary with a long life which renders a full color spectrum but has a slightly long strike and restrike time. Recommended for use in exterior applications where color CCTV is applied, or where exterior work is being performed. They employ sodium, thallium, indium, and mercury.

a. Advantages: Moderately long lamp life, 71 lumens per watt, natural colored light, low operating costs.

b. Disadvantages: High initial cost, does not restart immediately after a power failure.

37. FLUORESCENT LAMPS. These are large, elongated bulbs which provide a highlight output and have a recoverage light life of 7,500 hours. They have a higher initial cost than incandescent lamps, but a lower operating cost.

a. Advantages: Moderately long lamp life, 67 lumens per watt, low operating costs, even lighting from lamp with no hot spots.

b. Disadvantages: Higher initial cost than incandescent. Light control suitable for general areas, large fixture is required, light output is sensitive to ambient temperatures.

SECTION 6. KEY AND LOCK REQUIREMENTS AND CONTROL

38. REQUIREMENT. To satisfy the FAA's need for locking devices, the Best Universal Locks shall be the only keyed locking devices utilized for FAA owned and leased facilities.

a. Locking mechanisms manufactured by the Best Universal Company, Inc., shall be used by all FAA facilities to provide physical safeguards to ensure against malicious and willful damage to FAA equipment and other assets located in staffed and unstaffed facilities throughout the continental United States and overseas.

b. The FAA Standard Lock System must be keyed to a proprietary key way and key cutting codes designed solely for the use of FAA. All locks in the FAA system should have 7-pin removable and interchangeable cores which can be changed without the necessity of disassembling the entire core.

c. FAA facilities and/or operations that are using other than the FAA Standard Lock System shall replace existing key-operated locks with the FAA Standard Lock System as existing locks are due for replacement, become worn, broken, or compromised.

d. Best locks shall also be included in any lease agreements for facilities not under FAA control. The requirement for installation and retrofit of locks with the FAA Standard Lock System applies to FAA elements located in leased buildings.

39. ISSUANCE AND CONTROL OF LOCKS AND KEYS. An effective lock and key issuance and control system is essential to the safeguarding of property and controlling access. For effective control, accurate records shall be maintained and dated and semiannual physical inspections and inventories made. Keys shall be stamped "DO NOT DUPLICATE" prior to being issued.

40. KEY CONTROL OFFICIAL. A key control official shall be appointed in writing for every FAA facility having control over its own locking system. This official is responsible for the supply of locks and how they are stored, the handling of keys, records management, investigation of lost keys, ensuring hand receipts are signed for all keys issued and turned in, and the overall supervision of the key program at the facility.

41. RECORDS REQUIREMENTS. The key control official shall maintain a permanent record of the following:

a. Locks by number, showing:

(1) The location of each lock.

(2) The combination (if applicable). Combination records will be secured.

(3) Date of last combination change or core change.

b. Keys by number, showing:

(1) Location of each key (unissued key storage or hand receipts)

(2) Type of key combination of each key

(3) A record of all keys not accounted for.

(4) Record of whom each key was issued to by name.

42. ISSUANCE AND CONTROL PROCEDURES.

a. Keys, coded cards, and push-button combination shall be accessible only to those persons whose official duties require access to them.

b. Combinations to push-button locks shall be changed following the discharge, suspension, or reassignment of any person having knowledge of the combinations and at such other times as deemed appropriate, not to exceed 6 months for critical areas.

c. Issuance of keys shall be kept to a minimum and take place under constant key control supervision. The following requirements apply:

(1) Keys that are not issued shall be stored in a locked container that has been approved by the SSE when not in use.

(2) Access lists for persons authorized to draw keys shall be maintained in the key storage container.

(3) Key containers shall be checked periodically and all keys accounted for by documented semiannual inventories.

(4) Keys must be retrieved from personnel transferred, discharged, suspended, or retiring.

43. LOST AND UNACCOUNTED FOR KEYS AND ELECTRONIC ACCESS CARDS. When the results of the key inventories and inspections reveal that there are lost keys/access cards that cannot be accounted for, the key control custodian shall:

a. Report the loss of unaccounted keys/access cards to the SSE, together with a list of the areas to which the keys provide access. Lost access cards will be removed from the facility access control system.

b. Determine in coordination with the SSE and the facility manager the extent to which locks shall be recored, changed, or otherwise modified to prevent compromise of existing safeguards.

c. Locksets, keys, and access control cards shall be stored in locked containers or secured storage areas. (A locked office is not considered a locked container.)

APPENDIX 7. INTERIOR CONTROLS AND SECURITY PLANNING

1. OBJECTIVE. Good physical construction of a facility is the most important single measure to achieve security. The application of additional interior protective measures such as key control, secure lighting, alarms, CCTV, security containers, safes, and secured storage areas materially enhance the physical security of a facility. Security planning is needed to ensure all protective measures are coordinated and integrated. The criticality of any facility must be considered in the planning and design of new facilities and/or modifications of existing ones as stated in chapter 2. The following sections specify requirements that must be incorporated into all FAA facilities, new and existing.

SECTION 1. INTERIOR CONTROLS

2. INTERIOR MOVEMENT CONTROL. A positive personnel identification system shall be established and maintained in order to achieve required compartmentalization, preclude unauthorized entry, and facilitate authorized entry at personnel and vehicle control points. Positive personnel controls going into and within a facility are essential and must be established, monitored, and maintained. The following subparagraphs delineate the policy for personnel movement concerning the wearing of ID media. Examples of the forms referenced below can be found in FAA Order 1600.25. Deviations from this section must be approved by ACO-400 through coordination with the SSE.

a. All persons entering FAA facilities will have in their possession and will conspicuously wear issued identification badges on their outer clothing above the waist and below the neck.

b. All permanently assigned FAA employees will wear the FAA issued Identification Card, FAA Form 1681.1.3.

c. Personnel assigned to an ARTCC will be required to wear the ARTCC picture Identification Card, blue border, FAA Form 1600-38.

d. Personnel assigned to a CERAP facility will be required to wear the CERAP Picture Identification Card, brown border, FAA Form 1600-39.

e. Contractor personnel working for the FAA will be required to wear the Identification Card, DOT Form 1681.4.

3. VISITOR CONTROL AND SCREENING. Where required, visitors to FAA facilities will be required to wear the orange Identification Card, FAA Form 1600-50. These badges shall be worn at all times while on the facility and returned at the end of each day. The FAA visitor badges shall not be removed from FAA facility property. Any deviations from the official FAA Visitor Identification Card shall be requested from ACO-400 through the SSE.

4. VISITOR BADGE ACCOUNTABILITY. FAA Visitor Identification Cards, FAA Form 1600-50, are numbered and are accountable property. Facility management shall ensure inventories are taken on a daily basis and all missing badges shall be reported to the SSE.

SECTION 2. INTERIOR DOORS AND WALLS

5. GENERAL. Door construction is important as a primary safeguard against unauthorized access to restricted areas within the facility. These standards are to be used by the SSE and facility manager to assist them in establishing the appropriate safeguards.

6. DOOR FRAME AND CONSTRUCTION. Doors and frames providing access to any restricted area shall be of substantial metal or solid wood construction.

a. Doors shall be constructed of metal or metal clad and will be provided with FAA Best locks (7-pin).

b. Heavy-duty builder hardware shall be used throughout.

c. Electronic access control may become a required protective measure once the facility is assessed.

7. WALLS. Wall structures are normally not considered possible points of entry because of their usual solid construction. When a vulnerability is identified with a wall separating the FAA space from adjacent non-FAA office or areas, the SSE shall develop protective measures to reduce the vulnerability. In developing these measures, the objective will be to provide at the wall location a level of physical security that is at least commensurate with the value of the assets being protected. Protective measures which may be considered include, but are not limited to, the following:

a. Extending wall construction to ceiling or roof deck.

b. Constructing an expanded metal barrier to close the intervening space between the top of the existing wall and the ceiling deck.

c. When the primary concern is to detect unauthorized access attempts, rather than to deter or provide a substantial physical barrier, lightweight construction, such as plasterboard can also be used.

d. When lightweight materials are used, consideration shall be given to installation of an Intrusion Detection System (IDS) in the ceiling space to detect attempts at forced entry.

e. Covering the entire wall with 9-gauge expanded metal may be appropriate in some instances.

f. If the primary concern is that entry may be possible by forcible means without detection, the use of alarm sensors or vibration detection may be an effective solution.

8. ACCESS CONTROL. Controls and protective measures are established within a facility in order to protect employees and areas that are critical to the continued operation of the facility. A sudden disruption to the services provided by some FAA facilities could have disastrous consequences on air safety. Therefore, it is essential that area controls and other protective measures be established to protect our employees and facilities from physical damage or destruction. The protective measure outlined in this appendix are prescribed to deny admittance to unauthorized personnel.

a. Critical Areas. A critical area is an area to which entry shall be limited to authorized personnel and shall be designated when the following conditions exist.

(1) The area is critical to the continued operation of the facility and one which would be difficult to duplicate or restore. Examples:

(a) The power conditioning system (PCS) area.

(c) The air conditioning system control area servicing air traffic control computer equipment.

(c) Cooling towers.

(d) Emergency generator and associated equipment.

(e) Main power supplies.

(f) Main water supplies.

(g) Communications facilities such as air-ground ATC communications, radar data links, intrafacility ATC communications; emergency communications; demarcation areas; voice switched communications systems.

(h) Areas or rooms housing critical or key utilities.

(2) The area is one that requires controlled access by Public Law, national policy, or agency directive. Examples:

(a) Computer Rooms

(b) Areas processing certain types of financial and contract information and data.

(c) Areas processing and/or storing Privacy Act Information. (Privacy Act of 1974, FAA Order 1280.1)

(3) The area is one in which monies or sensitive negotiable forms are maintained. Examples:

(a) Government travel requests, and airline tickets (including ticket stock) in travel offices.

(b) Purchase Order Invoice Vouchers (SF-44) forms and 3rd party drafts.

(c) U.S. Government Transportation Request (SF-1169)

(d) Credit cards (e.g., AT&T, Government National Credit Cards, and credit cards issued to personnel.)

(e) Official passports.

(f) Funds in credit unions.

(g) Identification media blank forms in the issuing office.

(4) The area requires controlled access to preclude interference or disruption of the activities within the area. For example:

(a) ARTCC Air traffic control room floors.

(b) Airport traffic control towers.

(5) The area is used for the storage of valuable or sensitive equipment or data. Examples:

(a) Loan pools.

(b) Warehouse storage and processing areas.

(c) Mailrooms

(d) Medical offices.

b. Protecting Critical Areas. In establishing an effective system of internal area control for critical areas, the measures selected will be determined by the type of asset being protected and FAA requirements. Only personnel authorized shall be allowed entry into a critical area. At a minimum, these areas will be secured when assigned personnel are not present, all visitors shall be escorted within critical areas, and entrances into critical areas shall be posted with signage which states "RESTRICTED AREA – AUTHORIZED PERSONNEL ONLY." Below are additional means of controlling access into critical areas.

(1) Physical compartmentation from adjacent areas.

(2) Employee surveillance of the area.

(3) Use of high security locking devices to secure the room areas.

(4) Use of vault or strongroom construction.

(5) An effective system of personnel identification.

(6) Fixed guard post or receptionist at entrance to area.

(7) Use of electronic access control devices (e.g. card readers, digital scrambler pads, etc.)

9. EMERGENCY POWER FOR CRITICAL ALARMS. All alarm systems that alert for systems that are needed for the continued operation of the facility shall be provided with an emergency power supply. All alarm systems, CCTV monitoring devices, fire detection systems, entry control devices, etc., require emergency power sources.

SECTION 3. REQUIRED PLANNING

10. FACILITY SECURITY PLAN (FSP), OCCUPANT EMERGENCY PLAN (OEP), AND CONTINGENCY PLANS.

a. Facility Security Plan. The facility security plan (FSP) is a structured site specific security planning process which has the objective of developing a detailed written plan to assist the facility manager(s) in implementing adequate physical security protective measures and implementing safeguards against fraud, waste, and abuse.

b. Contingency Plans. Contingency Plans deal with FAA emergency operations and procedures for coping with the effects of a national emergency or major disaster. Complete information concerning emergency operations planning requirements is contained in FAA Order 1900.1, Emergency Operations Plan.

c. Occupant Emergency Plan. The OEP is defined by the Federal Property Management Regulation (FPMR) as "...a short term emergency response program that establishes procedures for safeguarding lives and property during emergencies in particular facilities." The OEP has two components, the first is the development of procedures to protect life and property, the second is the formation of an occupant emergency organization within each office or facility, comprised of employees designated to undertake and perform the specific tasks outlined in their OEP.

11. OEP RESPONSIBILITY. The FPMR places responsibility for managing emergencies in a federally owned or leased facility upon a "Designated Official, " who is "a designee selected by mutual agreement of occupant emergency officials." This person is responsible for developing, implementing, and maintaining an OEP as defined in the FPMR. The designated official's responsibilities include establishing, staffing, and training an Occupant Emergency Organization with FAA employees. In each staffed office or facility under FAA control, the facility manager or his or her designated representative shall be appointed as the "Designated Official." An alternate designated official shall also be appointed. The Designated Official shall request the assistance of the SSE in the formulation of the OEP.

a. FAA offices in GSA-Controlled Facilities. GSA is responsible for providing standard protection services for properties under its control by coordinating a comprehensive Occupant Emergency Program.

b. Terrorist Demands, Threats, or Actions. The FAA OEP shall contain specific guidance on planning and action to be taken in response to demands, threats, or actions by terrorist groups.

12. FACILITY SECURITY PLAN. The Facility Manager is responsible for the development and implementation of the FSP at his or her facility. Where there are multiple FAA managers located in a single facility, the development of the FSP shall be a joint responsibility.

a. The SSE is responsible for advising and assisting FAA facility managers in the development of an FSP for specific facilities.

b. An FSP is required at all staffed FAA facilities. However, because of the number, differing security level designations, and variety of missions of FAA facilities, the size and content of a site specific FSP may vary from one facility to another. In most instances, smaller facilities will have less complex security programs and systems. This section contains guidance on required items that must be

included in all FSP's. A sample format for a FSP is included in appendix 3. The final responsibility to develop and implement an FSP shall be achieved through coordination between the SSE and the appropriate facility manager(s).

c. The coordination between the SSE and the FAA facility manager concerning the FSP normally will take place at the time of the physical security assessment and will be a critical factor in determining whether physical security accreditation will be granted for the facility. A determination as to the effectiveness of a facility FSP will be included in each assessment, inspection, and accreditation evaluation performed by the SSE. The facility manager(s) shall develop the FSP with the advice and assistance of the SSE.

d. The FSP is a physical security plan and it must be tailored to the physical security needs of each facility. It must also be capable of representing management's interests in implementation of physical security protective measures. The FSP and OEP if the facility does not have one all inclusive plan, must be tested annually.

e. A basic element of the FSP is a security and/or response force capable of ensuring enforcement of established security measures and procedures.

f. Established physical security measures and systems such as barriers, protective lighting, communications, CCTV, electronic access control systems, and other measures as appropriate will be incorporated into the plan to increase the effectiveness of the physical security measures that are in place. The selection, type, and use of physical security protective measures is the responsibility of facility designers, the SSE, and facility managers working in close coordination.

g. The FSP shall contain specific guidance on:

(1) Planning and actions to be taken in response to bomb threats and demands, threats, or actions, by terrorist groups as specified in this order and facility contingency, occupant emergency, and emergency operations plans.

(2) Procedures for liaison between the facility and other support agencies and services, to include, local police and fire departments, emergency medical response, explosive ordinance disposal teams, state and Federal law enforcement authorities.

(3) If contract guard services are being used, the plan should clearly identify the jurisdictional authority of the FAA security force. Additionally, the FSP will generally address the contract security guards basic concerns such as responsibilities, duties, and overall integration into a facility's security program.

(4) The FSP should contain specific guidance on access controls, visitors, deliveries of mail, equipment and supplies, facility parking, designation of critical areas, information systems security, document controls, and any other area that affects the overall level of physical security at an FAA facility.

h. Standards of security. Security standards established by this order, as well as standards included in the orders and directives listed in appendix 2, shall be used in planning a facility security management program and the development of the facility FSP.

13. INFORMATION SECURITY. All information protected under the Privacy Act shall be controlled and protected in accordance with FAA Order 1280.1. For Official Use Only (FOUO) and classified information shall be controlled and protected in accordance with FAA Order 1600.2.

SECTION 4. SECURITY PLANNING

14. ESTABLISHMENT OF BUILDING SECURITY COMMITTEE (BSC) AND FACILITY SECURITY COORDINATOR (FSC). The facility manager shall ensure that a BSC is formed. The Committee should consist of representatives from all other organizations or agencies if they are collocated. Additionally, the facility manager shall assign a FSC. The FSC should be part of the BSC and would be responsible for: being the facility point of contact for physical security assessments and inspections, evaluate, and apply the appropriate minimum protective measures developed for the facility and determine in coordination with the BSC the minimum requirements and feasibility of implementation of identified protective measures.

a. The FSC/BSC should establish a liaison with appropriate law enforcement agencies.

b. The FSC should establishprocedures for intelligence receipt and dissemination.

15. CONTRACTOR BACKGROUND CHECKS. All contract personnel shall have a background check as required by FAA Order 1600.1. It is the responsibility of the facility manager to ensure that all contract personnel assigned to his/her facility are in compliance with Order 1600.1 by contacting the SSE with notification of new contractor personnel.

16. SECURITY AWARENESS TRAINING. Annual security awareness training shall be provided to all personnel assigned to an FAA facility. Documentation of such training (class rosters, briefing sign-in sheets, read and initial files, etc.) must be maintained at the facility. Topics to be covered include:

a. ID display policy (if required.)

b. Vehicular and parking safety policies.

c. After hours access.

d. Reporting suspicious persons or activities

e. Visitor policy.

f. Bomb threats.

g. Information security.

h. Security Hazard Reporting.

i. Access into controlled areas.

j. Facility Security Plan to include the OEP.

k. Local threats and vulnerabilities.

17. BOMB THREATS AND INCIDENTS.

a. Incidents and Reactions. Bomb incidents are actual placement, or detonation of an explosive, incendiary, corrosive, or other destructive device.

b. Threats and Reactions. Bomb threats are communication of a threat transmitted by word or deed. The threat may be made in person, by telephone, or passed by note or letter.

(1) **Telephonic Bomb Threat.** Each employee is responsible to ensure that his/her telephone is equipped with FAA forms 1600.52 (envelope) and 1600.53 "Bomb Threat Card." Each card includes a checklist about the phone call and a recommended list of questions to ask the caller. The call receiver should attempt to keep the caller on the line, should not put the caller on hold, ask them to wait, call back, or transfer the caller to another phone. When the call is received:

(a) Retrieve and use the bomb threat card, notify Someone Else. If the caller is staying on the line, write a quick note, if possible, and pass it to a co-worker: "BOMB THREAT - GET HELP." Concentrate your attention on the call. Use the questions on the checklist. The most important questions to ask are: (1) Where is the bomb? (2) When will the bomb go-off? (3) What type of bomb is it (dynamite, plastic, incendiary, etc..)? When establishing the time at which the bomb will detonate, try to get the actual time; i.e. 4:00 pm, rather than a general statement such as "30 minutes."

(b) During the call try to take notes of what the caller says, facts about the caller, and the phone call itself as noted on the card: the callers emotional state, background noises, etc... Make notes on the card if necessary, but it is generally better to make notes on a separate sheet of paper.

(c) After the call, immediately contact your supervisor/manager. Notification shall be made to the FAA Regional Operations Center (ROC) and Servicing Security Element (SSE). Consolidate your notes, and write down everything you can remember about the call. Use the checklist on the card to prompt your memory, but don't limit your observations to the checklist. Include your impressions, "gut-feelings," and any and all facts no matter how seemingly unimportant.

(2) Written Bomb Threat. When a note or letter is received that contains a threat of any nature, immediately put the paper down and handle as little as possible from that point on. Do not touch the paper further, do not re-fold it, or put it back in the envelope. Do not abandon the paper, show the paper to curious persons, or allow anyone else to touch it. Slide the paper and envelope, if any, into a file folder or large envelope without touching it. Do not write on the envelope or folder once the paper is inserted. Secure the folder or envelope in a locked drawer or cabinet. Make the same notifications as in paragraph above. Make notes on a separate sheet of paper including all details and circumstances of how you came into possession of the paper.

(3) Personal Contact. Notify the Supervisor on duty immediately.

(a) Keep the person making the threat, or indicating knowledge of a threat, under surveillance until relieved by competent authority.

(b) Note the sex, age, height, weight, coloring of eyes, skin, hair, clothing, and any unusual characteristics.

(c) Note the make, model, color, and license number of vehicle if used by a person leaving the scene.

(4) Letter and Parcel Bombs. Every employee who receives and processes mail shall have a Letter and Parcel Bomb Recognition Checklist available at his/her work station. Whenever a suspected letter or parcel bomb is received do not immerse the article in water, place in a trash can or other container. Above all, do not cut, tear, or press on the outer covering. See appendix 3 for example of suspect letter and package indicators. Take the following actions:

(a) Note the complete address and any markings on a separate sheet of paper, then

(b) Isolate the Item. That is, place the item in a location where other employees will not open or disturb the item.

(c) Contact the ROC and SSE. Describe the package, what your suspicions are and why, where the package is presently located, your name and phone number.

(d) Contact the Addressee. The person or office the item is addressed to may be expecting the package, or may be able to help determine who may have sent it, or what may be in it.

(e) Contact the Sender. If the sender is included in the return address, they may be able to verify they sent a package meeting the description of the package you have, and identify its' contents.

APPENDIX 8. LOSS AND THEFT PREVENTION

SECTION 1. ACCOUNTABLE EQUIPMENT CATEGORIES

1. **Sensitive items regardless of price**

    a. Ammunition

    b. Firearms

2. **Sensitive items ($500.00 or above)**

    a. Audio visual equipment (asset class 13); e.g.,

        (1) Photographic/projection/development equipment (cameras, digital cameras, etc.)

        (2) Recording equipment

        (3) Printing/duplicating equipment/facsimile machines

        (4) Television/video recording equipment

    b. Automated data processing equipment (asset class 17); e.g.,

        (1) Central processing units (CPU's)

        (2) Computer monitors

        (3) Computer printers/monitors

        (4) Computer peripherals

        (5) Laptop/Notebook computers

    c. Test equipment (asset classes 62 and 63); e.g.,

        (1) Portable test equipment

        (2) Rack-mounted test equipment

    d. Portable telecommunications equipment (asset class 64); e.g.,

        (1) Telephones

        (2) Pagers

        (3) Cellular Telephones

(4) Portable and installed communications equipment

3. Accountable property (all personal property costing $2,500.00 or more)

Each headquarters, regional, or center property manager retains the right to: (1) lower the dollar threshold of an item or (2) add specific items for their area of control or a specific site, as appropriate to ensure government property under their control is safeguarded. However, such decisions must be based on specific problems associated with an item or site and be documented.

APPENDIX 9. REQUIREMENTS FOR NEW FACILITY CONSTRUCTION, RENOVATION, AND LEASED SPACE

SECTION 1. PLANNING AND DESIGN

1. GENERAL GUIDELINES FOR FACILITY TYPES. In addition to the protective measures identified in chapter 3, the measures depicted in table 6-1 and defined in table 6-1a must be implemented.

2. GENERAL CONSIDERATIONS.

a. Selecting space. In facilities housing multiple organizations, avoid separating or scattering offices throughout the building. Wherever possible, locate the FAA spaces on the upper rather than the lower floors. Wherever possible, collocate the space with other FAA elements on the same floor(s). Access controls shall be emphasized. Attempt to obtain leased space with entities having similar security needs. Do not locate FAA personnel in facilities housing high-risk agencies such as (Drug Enforcement Agency (DEA), Bureau of Alcohol, Tobacco and Firearms (ATF), Federal Bureau of Investigation, (FBI), Internal Revenue Service (IRS), etc.

b. Obtaining protective services. Wherever possible, utilize protective forces provided by GSA/FPS or the host agency. Establish liaison with local law enforcement advising them of the criticality of the facility, security features and systems, administrative and operational hours, and points of contact for both general business and in emergencies.

c. As a planning goal, all design and construction projects will be reviewed to incorporate current technology and blast standards. Immediate review of ongoing projects may generate savings in the implementation of upgrading to higher blast standards during the design and planning stage. Establishing an exterior street set-back of 300 feet and an interior set-back of 100 feet. is required.

d. For all FAA facilities which have employee leased parking, the lease should include provisions for security controls. Security guard services should be included in parking leases whenever possible.

3. PERIMETER. The perimeter of a facility is the outermost point of protection controlled by the facility/office/activity. The perimeter is normally considered to be at the property line, security fenceline, or at the furthermost controlled point outside the facility exterior. However, at some facilities, such as those located within a larger building, the perimeter may be considered the exterior of the building, or the access point onto a floor from a stairwell or elevator lobby. The perimeter shall be defined by signs, fencing, gates, doors, or other barrier(s) including natural protection.

4. PARKING. The control of vehicular access to a facility can facilitate the highest level of deterrence. For new construction of FAA owned facilities, parking shall not be allowed within 100 feet of the building exterior.

5. EXTERIOR SECURITY. The area between the perimeter and the building exterior, including parking areas, must be evaluated for the potential for hostile intruders to conceal themselves or lethal devices within the buffer zone. Lighting during hours of darkness must be evaluated.

6. PERSONNEL ENTRANCES. The facility may be designed with a number of personnel entrances to enable maximum access when needed. Operational configuration shall limit the number of in-use entrances to be consistent with the minimum necessary for normal operational needs.

a. Main Entrances. Design as a vestibule configuration with lockable but normally unsecured outer doors, and lockable but normally unsecured or electronic access system controlled inner doors. Entrances shall be designed so that visitors must be met by a secretary, receptionist, guard officer or other authorized person before proceeding further. If facility security system controls are located within this reception area, they shall be installed in a secure cabinet designed and constructed to withstand manipulation and/or physical attack.

b. Secondary Entrances. In a large, critical facility, it may be necessary to incorporate one or more secondary entrances. These are entrances necessary for movement of staff, deliveries, etc., into and out of the facility. Secondary entrances must not be unsecured unless continually staffed. Secondary entrances must be controlled by key or electronic access system.

c. Emergency and Utility Exits. Exterior doors designed to be used only in special circumstances, or as exits during emergencies, shall be designed without external opening hardware, door position indicator, and if equipped shall be monitored in the Intrusion Detection System. Audible warning horn should be connected to the door to annunciate if opened.

d. Shipping and Receiving Points. Shipping and receiving areas shall be secured whenever unattended. Delivery companies shall be advised that deliveries may be received only during normal business hours, and that parcels, packages, or other deliveries may not be left outside the facility, on freight docks, or on the property but rescheduled for delivery the next normal working day. Specific procedures will be covered in the facility security plan.

e. Windows. Where required, windows shall be constructed of laminated safety glass, chemically tempered glass, acrylic, or polycarbonate

7. CHILD CARE CENTERS. When obtaining leased space or construction of a new facility involving a child care center, consideration shall be given whether to locate the child care center within or outside the facility perimeter. All child care centers shall be constructed in accordance with appendix 11.

APPENDIX 10. PHYSICAL SECURITY ASSESSMENT AND INSPECTION OVERVIEW

1. **PHYSICAL SECURITY OVERVIEW.** Figure A10-1, Physical Security Overview, provides a visual summary of the complete assessment and inspection process that is used for the FAA facility security management program.

2. **PHYSICAL SECURITY ASSESSMENT OVERVIEW.** Figure A10-2, Physical Security Assessment Overview, provides a visual summary of the assessment process used to evaluate FAA facilities. In addition, Figure A-10-2a, Physical Security Assessment Overview is a chart developed to provide an outline of the details within the assessment process. The SSE shall accomplish each of the steps and items depicted in Figures A10-2 and A10-2a. The following is a narrative summary of that Figure A10-2.

a. Assessment Objectives. The assessment is planned and conducted by the SSE and consists of an on-site examination of the facility, the local threats and vulnerabilities that might exist, and the overall risk level to the facility. The SSE shall notify the facility manager and the appropriate LOB management of the planned assessment. Participation in the assessment will be at the discretion of the LOB management. Physical security assessments provide an evaluation of meaningful threats, vulnerabilities, overall risk level assigned, prioritized protective measures required and recommended with estimated costs for each protective measure.

b. Assessment Requirements. FAA Order 1600.69 requires a physical security assessment of all staffed facilities and is the basis for determining facility accreditation. An assessment cadre shall consist of several team members selected by the SSE. Team members may be members from the SSE staff and applicable LOB. During the physical security assessment, a myriad of security orders such as 1600.54, 1600.1, 1600.2, 1600.8, and 1600.25 will be used in conducting the assessment.

c. Assessment Preparation. Planning for a physical security assessment must begin well before the actual assessment date. The SSE conducting the assessment shall coordinate with facility managers and LOB FSMP focal point(s), notifying them of the assessment date, areas to be evaluated, assessment team composition, length of stay, facility security point of contact(s), and establish an in-brief schedule. The SSE will:

(1) Review the facility's security plan. By reviewing the FSP, a determination can be made as to what levels of security are required at the facility as well as the type of electronic and mechanical security aids that are present.

(2) Determine the facility mission. By evaluating the facility's mission, a determination can be made as to the criticality of the facility to the FAA and the National Airspace System (NAS). The determination of criticality shall be made by the SSE in conjunction with the LOB.

(3) Retrieve facility blueprints. By reviewing applicable facility blueprints, a determination can be made as to numbers of exterior doors, new construction, location of critical systems or equipment, etc.

(4) Review previous FSRS reports. Reviewing previous reports can be beneficial in identifying previous deficiencies, facility weak areas or the overall attitude of assigned personnel to security requirements and initiatives. SSE's will coordinate and where necessary provide copies of previous inspection reports, with LOB focal points in reviewing past assessments and reports.

(5) Acquire Intelligence data on criminal and terrorist activity. This data is essential in determining the threat levels at a particular facility. Data shall be collected from ACI as well as the local law enforcement jurisdictions servicing the facility. Coordinate with local authorities in acquiring such intelligence data as crime statistics and information on known terrorist groups residing in the area.

(6) Determine the closest local, state, or federal Emergency Services Team such as SWAT, FBI Hostage Rescue Team, explosive ordinance disposal (EOD), bomb dogs, medical and fire response units, etc., serving the facility.

d. Assessment Entrance Briefing. The entrance briefing is critical as it sets the tone for the entire assessment. Be professionally courteous, establish rapport, but stick to the point. Establish your objectives, identify key personnel at the facility, ask for any facility concerns, request a work area within the facility, and establish an exit briefing schedule.

e. Assessment and Exit Briefing. The assessment must be organized and have specific goals and objectives with defined time lines for accomplishment.

(1) Organize on-site effort into work functions and tasks. Depending on the size of the assessment team, it is normally advisable to start at the facility perimeter and work inwards. This is not a concern with large teams. One member of the team shall contact the public safety agencies having jurisdiction for the facility.

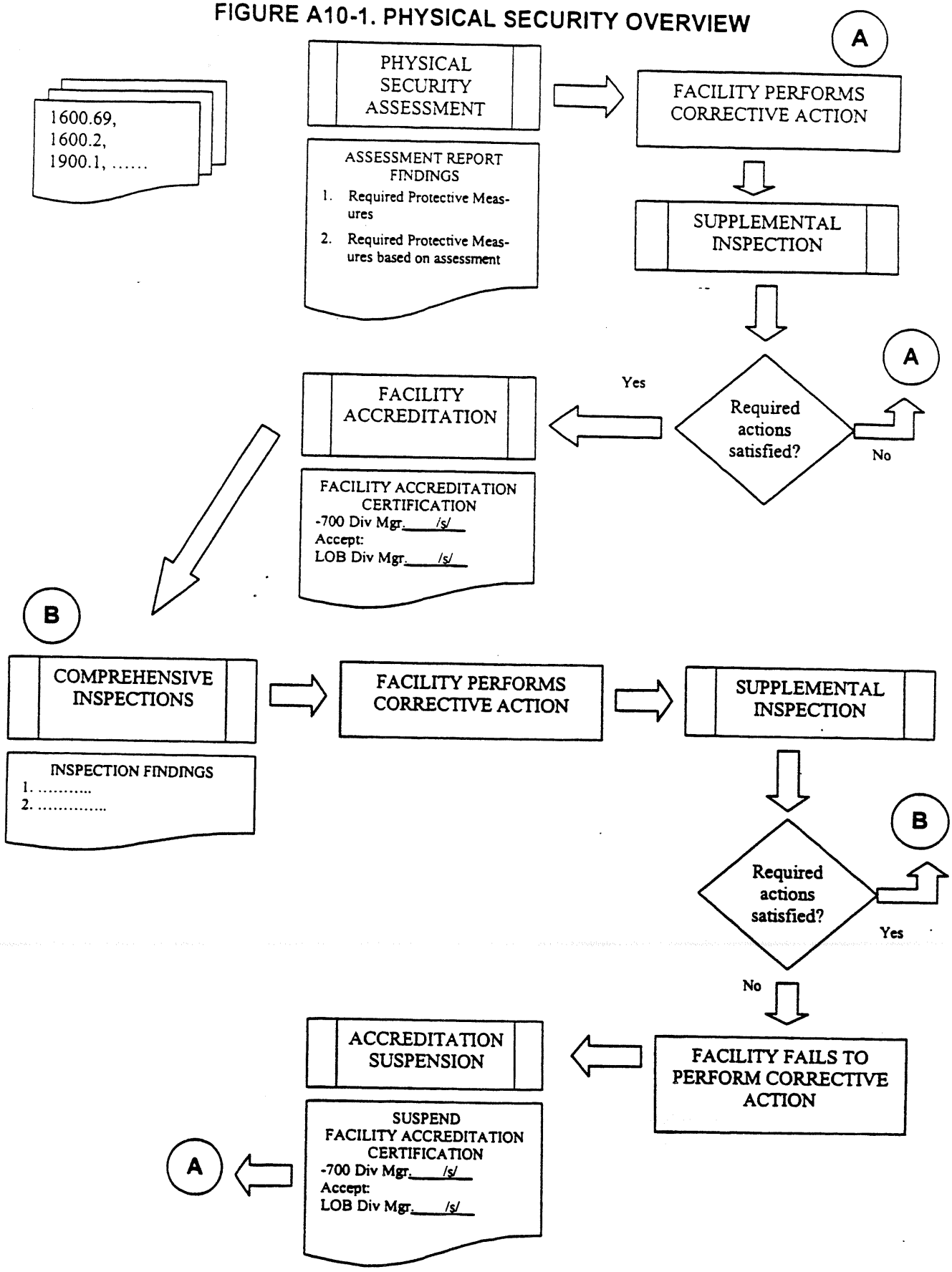
(2) Evaluate the facility. Determine if the facility meets the functional security requirements identified in Chapter 3 for this type and size of FAA facility. Evaluate known threats (crime statistics, interviews with law enforcement, terrorist activity, etc.), against in-place physical security equipment and procedures. Determined shortfalls are classified as vulnerabilities.

(3) Determine Risk and Protective Measures. Where there is a threat and identified vulnerabilities, you have risk. If the risk level is determined to be high, the SSE must determine what protective measures are to be implemented, to include cost.

(4) Exit briefing. In preparation for the exit briefing, collect, organize, and review all the assessment team findings. Provide the facility manager with all deficiencies that were identified. Relate that you and your team are available to assist the facility in correcting identified deficiencies.

f. Assessment Follow-up. Follow through on any IOU's or consultant support that was promised to the facility manager. Complete the Executive Summary of the physical security assessment and include all findings along with the estimated costs for implementing required protective measures. Dependent on the types of findings that were identified, plan for a supplemental inspection to verify correction of identified deficiencies. Track the completion of required facility actions as they are completed in FSRS. Prior to the supplemental inspection, again offer your assistance to assist the facility in correcting identified deficiencies.

FIGURE A10-1. PHYSICAL SECURITY OVERVIEW



3. PHYSICAL SECURITY COMPREHENSIVE INSPECTIONS OVERVIEW. Figure A10-3, Physical Security Comprehensive Inspection Overview, provides a visual summary of the inspection process used to evaluate FAA facilities. In addition, Figure A-10-3a, Physical Security Comprehensive Inspection Overview, is a chart developed to provide an outline of the details within the comprehensive inspection process. The comprehensive inspection process is essentially a variation of the assessment process with less emphasis on analysis of vulnerability, threat, and overall facility risk. The SSE shall accomplish each of the steps and items depicted in Figures A10-3 and A10-3a.

4. PHYSICAL SECURITY ACCREDITATION AND SUSPENSION OVERVIEW. Figures A10-4, Physical Security Accreditation Overview, and A10-5, Physical Security Suspension of Accreditation Overview, provides a visual explanation of FAA facility accreditation certification and suspension of facility accreditation. In addition, Figures A10-4a, Physical Security Accreditation Overview, and A10-5a, Physical Security Accreditation Overview, are charts developed to provide an outline of the details within the accreditation certification and suspension process. The SSE shall accomplish each of the steps and items depicted in Figures A10-4, A10-4a, A10-5, and A10-5a.

5.-19. RESERVED.

FIGURE A10-2. PHYSICAL SECURITY ASSESSMENT OVERVIEW

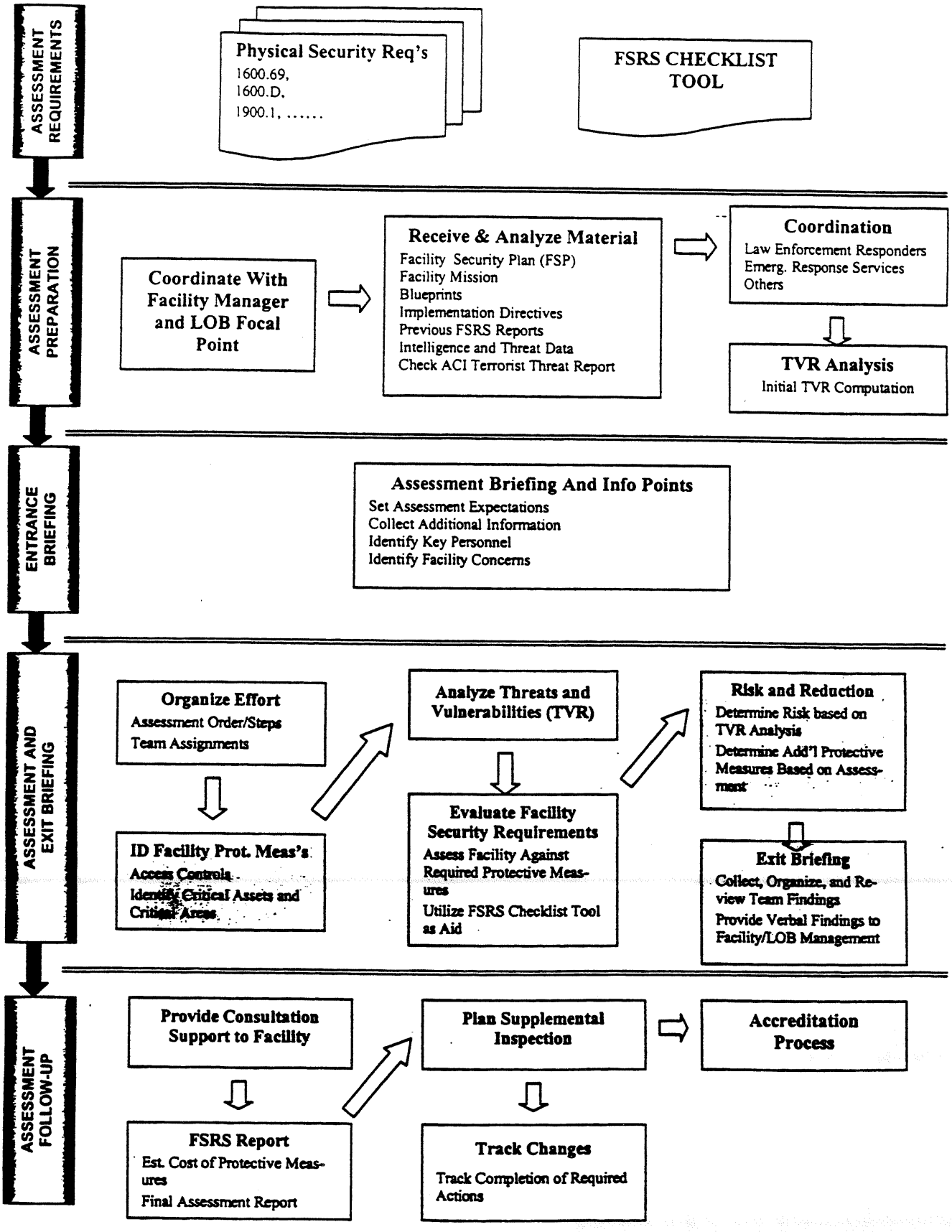


FIGURE A10-2a. PHYSICAL SECURITY ASSESSMENT OVERVIEW

ASSESSMENT REQUIREMENTS

- FAA Order 1600.69
- Other Security Related Orders
- FSRS Checklist Tool

ASSESSMENT PREPARATION

- Communicate with Facility Manager
- Receive and Analyze:
  - Facility Physical Security Management Plan (FPSMP)
  - Facility Mission
  - Blueprints
  - Implementation Directives
  - Previous FSRS Reports (Surveys/Inspections)
  - Intelligence and Threat Data
  - Check ACI Terrorist Threat Report
- Coordinate with:
  - Law Enforcement
  - Emergency Response Services
  - Others
- Begin TVR Analysis

ASSESSMENT ENTRANCE BRIEFING

- Set Assessment Expectations
- Collect Additional Information
- Identify Key Personnel
- Identify Facility Concerns

FIGURE A10-2a. PHYSICAL SECURITY ASSESSMENT OVERVIEW (cont.)

ASSESSMENT AND EXIT BRIEFING

- Organize On-Site Effort Into Work Functions and Tasks
  - ➢ Order of Events/Steps (Outside – In)
- Identify Current Facility Protective Measures
  - ➢ Identify Critical Areas and Critical Assets
- Conduct Analysis of Threats and Vulnerabilities (TVR Analysis)
- Evaluate Facility Physical Security Requirements
  - ➢ Facility vs. Required Protective Measures
  - ➢ Utilize FSRS Checklist Tool (as an Aid)
- Determine Risk and Risk Reduction Measures
  - ➢ Determine Risk Based on TVR Analysis
  - ➢ If Risk is High – Determine Required Protective Measures Based on Evaluation
- Provide Exit Briefing
  - ➢ Collect, Organize, and Review Team Findings
  - ➢ Provide Verbal Summary of Findings

ASSESSMENT FOLLOW-UP

- Provide Consultation Support to Facility Manager
- Complete FSRS Assessment Report
- Estimate Cost of Required Protective Measures
- Plan for Supplemental Inspection
- Track Completion of Required Actions

FIGURE A10-3. PHYSICAL SECURITY COMPREHENSIVE INSPECTION OVERVIEW

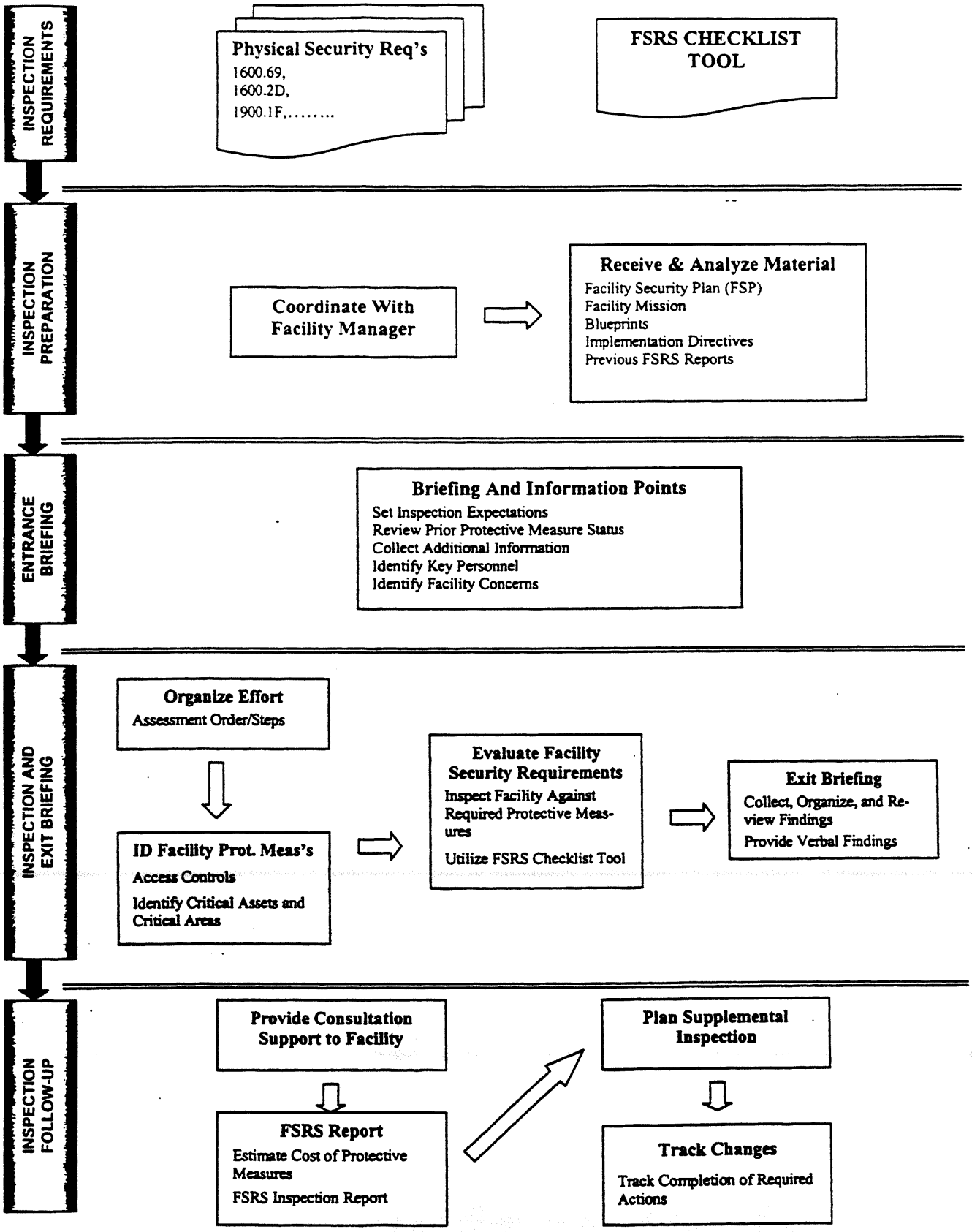


FIGURE A10-3a. PHYSICAL SECURITY COMPREHENSIVE INSPECTIONS OVERVIEW

INSPECTION REQUIREMENTS

- FAA Order 1600.69
- Other Security Related Orders
- FSRS Checklist Tool

INSPECTION PREPARATION

- Coordinate with Facility Manager
- Receive and Analyze:
  - Facility Security Plan (FPSMP)
  - Facility Mission
  - Blueprints
  - Implementation Directives
  - Previous FSRS Inspection and Assessment Reports

INSPECTION ENTRANCE BRIEFING

- Set Inspection Expectations
- Review Prior Protective Measure Status
- Collect Additional Information
- Identify Key Personnel
- Identify Facility Concerns

INSPECTION AND EXIT BRIEFING

- Organize On-Site Effort Into Work Functions and Tasks
  - Order of Events/Steps (Outside – In)
- Identify Current Facility Protective Measures
  - Identify Critical Areas and Critical Assets
- Evaluate Facility Physical Security Requirements
  - Facility vs. Required Protective Measures
  - Utilize FSRS Checklist Tool
- Provide Exit Briefing
  - Collect, Organize, and Review Findings
  - Provide Verbal Summary of Findings

FIGURE A10-3a. PHYSICAL SECURITY COMPREHENSIVE INSPECTIONS OVERVIEW (cont.)

INSPECTION FOLLOW-UP

- Provide Consultation Support
- Complete FSRS Inspection Report
- Estimate Cost of Required Protective Measures
- Plan for Supplemental Inspection
- Track Completion of Required Actions

FIGURE A10-4. PHYSICAL SECURITY ACCREDITATION OVERVIEW

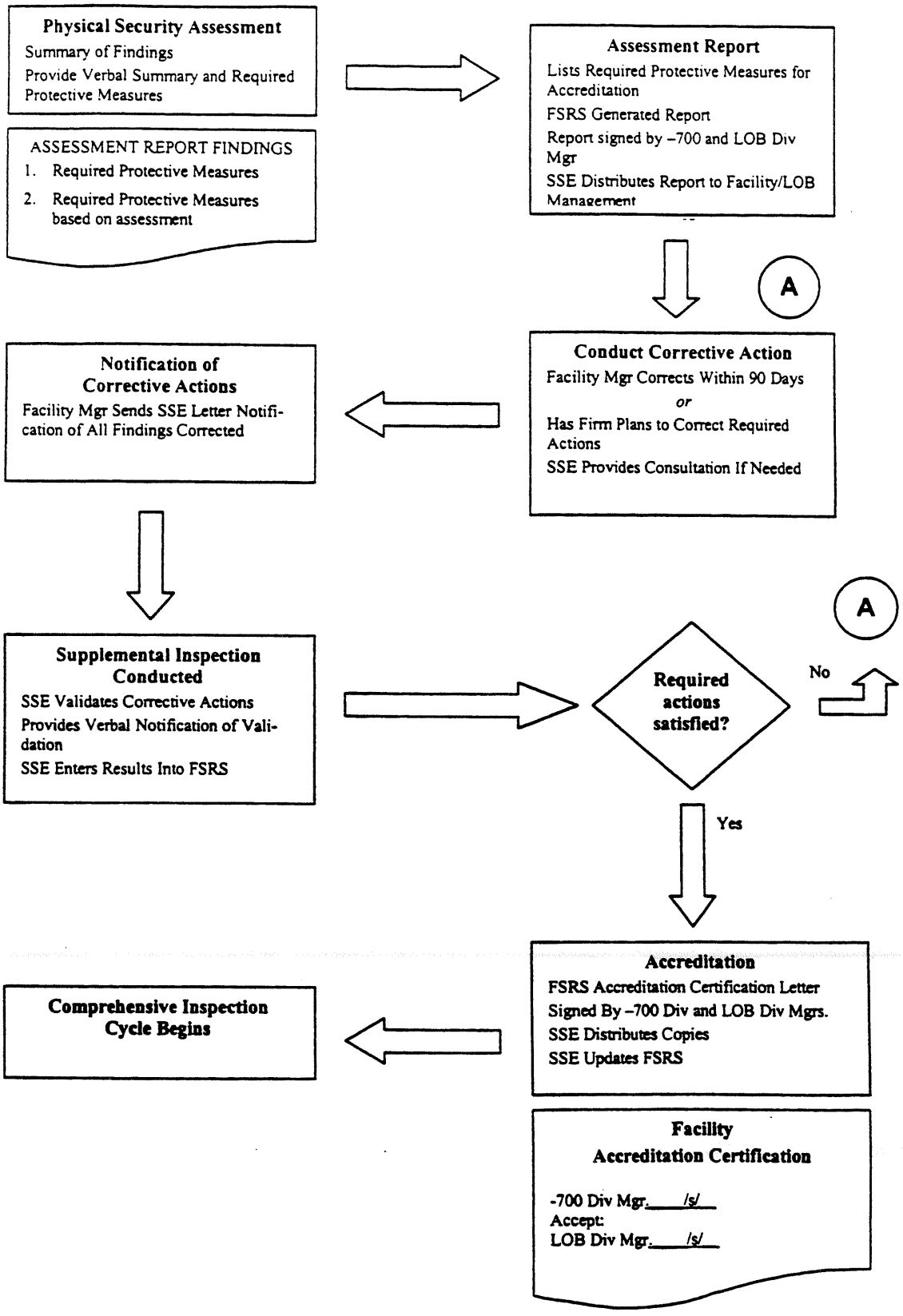


FIGURE A10-4a. PHYSICAL SECURITY ACCREDITATION OVERVIEW

PHYSICAL SECURITY ASSESSMENT

- SSE Conducts Physical Security Assessment of Facility
- Develops Summary of Findings of Required Protective Measures
- SSE Provides Facility Manager with Exit Briefing
- SSE Provides Verbal Notification of Findings

ASSESSMENT REPORT

- Enumerates Required Protective Measures Needed For Accreditation
- FSRS Generates Report
- Assessment Report Is Signed Off By –700 Division
- SSE Provides LOB FSMP/Div. Mgr and Facility Manager the Assessment Report

CONDUCTS CORRECTIVE ACTION

- Facility Manager Takes Corrective Action Within 90 Days
- Or Have Firm Plans In Process To Correct The Problems Within A Reasonable Period Of Time
- SSE Provides Consultation Support if Requested

NOTIFICATION OF CORRECTIVE ACTIONS

- Facility Manager Notifies Via Letter When All Findings Are Implemented
- SSE Must Conduct Supplemental Inspection and Issue Accreditation Letter within 45 days

SUPPLEMENTAL INSPECTION CONDUCTED

- SSE Validate Corrective Actions
- SSE Provides Verbal Notification of Validation
- SSE Enters Satisfactory Validation Results Into FSRS

FIGURE A10-4a. PHYSICAL SECURITY ACCREDITATION OVERVIEW (cont.)

FACILITY ACCREDITATION CERTIFICATION

- FSRS Develops FAA Facility Accreditation Certification Letter
- Accreditation Certification signed off by –700 Div. And LOB Div. Mgrs.
- SSE Retains Original Accreditation letter in –700 files
- SSE Sends copy of Accreditation to:
  - LOB FSMP
  - LOB Div Mgr
  - Facility Manager
  - ACO-400
- SSE Enters Accreditation Update into FSRS

COMPREHENSIVE INSPECTION CYCLE BEGINS

FIGURE A10-5. PHYSICAL SECURITY SUSPENSION OF ACCREDITATION OVERVIEW

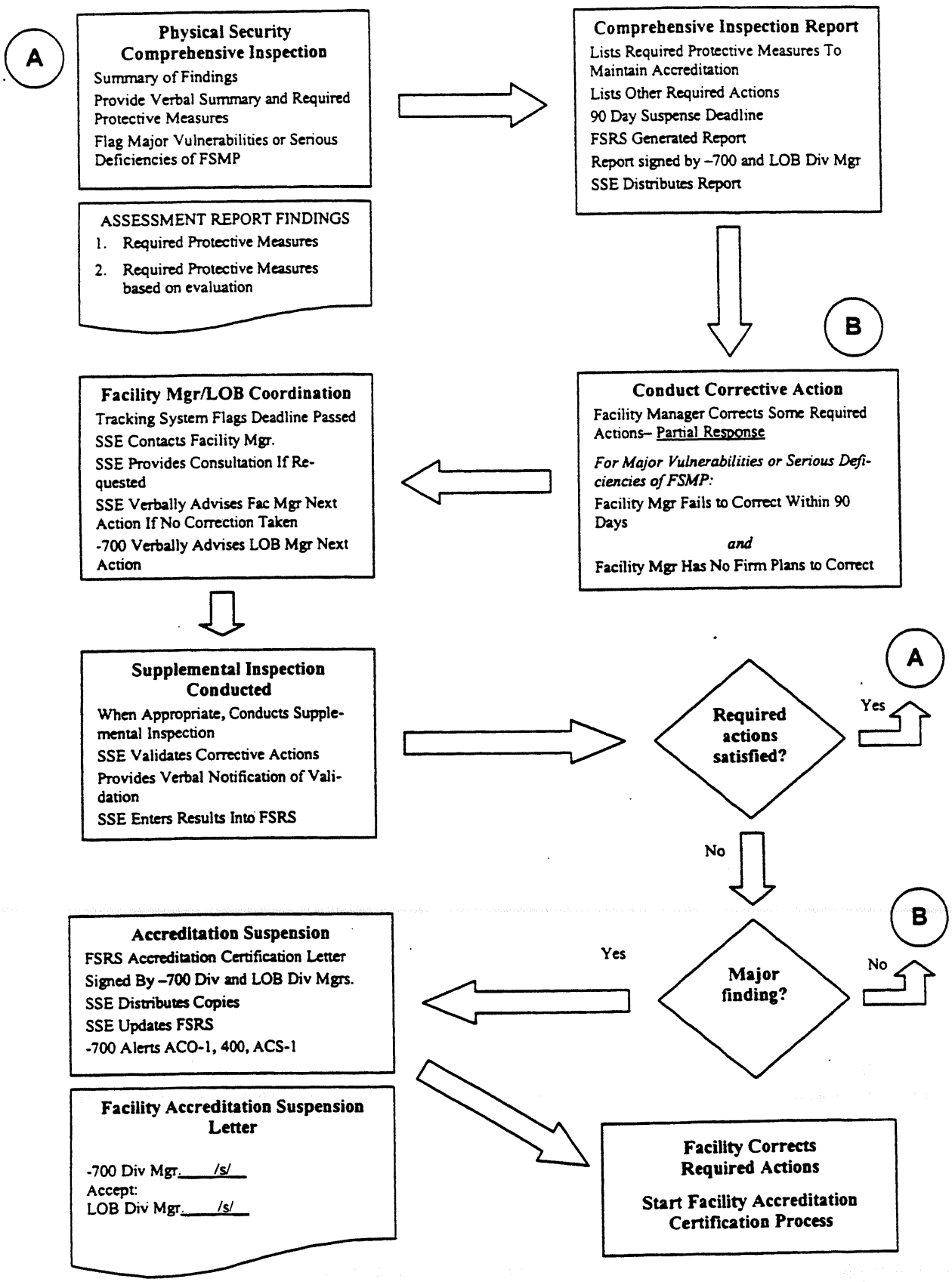


FIGURE A10-5a. PHYSICAL SECURITY SUSPENSION OF ACCREDITATION OVERVIEW

PHYSICAL SECURITY COMPREHENSIVE INSPECTION

- Develops Summary of Findings of Required Protective Measures
- SSE Provides Facility Manager with Exit Briefing
- Verbal Notification of Findings to Facility Manager
- Flag Major Vulnerability or Serious Deficiency of FSMP
  - changes in the environment
  - mission changes
  - increased threat levels
  - new construction
  - other

COMPREHENSIVE INSPECTION REPORT

- Lists Required Protective Measures Needed To Maintain Accreditation
- Lists Other Required Protective Measures
- Imposes 90 Day Suspense Deadline
- FSRS Generates Report
- Inspection Report Is Signed Off By –700 Division Manager
- SSE Provides LOB Div. Mgr and Facility Manager the Inspection Report

IMPLEMENTS CORRECTIVE ACTION

- Facility Manager Corrects Some Required Actions – Partial Response
- Facility Manager Fails To Correct Within 90 Days
- Facility Manager Has No Firm Plans In Process To Correct The Problems Within A Reasonable Period Of Time

FACILITY MANAGER AND LOB MANAGER COORDINATION

- Tracking System Flags 90 Day Deadline Passed
- SSE Contacts Facility Manager
- SSE Provides Consultation Support if Requested
- SSE Appraises Facility Manager of Next Action If No Correction Taken
- -700 Communicates to LOB Division Manager of Next Action

FIGURE A10-5a. PHYSICAL SECURITY SUSPENSION OF ACCREDITATION OVERVIEW (cont.)

SUPPLEMENTAL INSPECTION CONDUCTED

- When Appropriate Schedule and Conduct Supplemental Inspection
- SSE Validates Corrective Actions
- SSE Provides Verbal Notification of Validation
- SSE Enters Satisfactory Validation Results Into FSRS

FACILITY ACCREDITATION SUSPENSION

- FSRS Develops FAA Facility Accreditation Certification Suspension Letter
- Accreditation Suspension signed off by –700 Division Manager
- SSE Retains Original Accreditation Suspension Letter in –700 files
- SSE Sends copy of Accreditation Suspension Letter to:
  - LOB Div Mgr
  - Facility Manager
  - ACO-400
- SSE Enters Suspension Accreditation Update into FSRS
- -700 Reports Suspension to ACO-1, 400, ACS-1

FACILITY MANAGER CORRECTS REQUIRED ACTION

START FACILITY ACCREDITATION CERTIFICATION PROCESS

APPENDIX 11. CHILD CARE CENTER SECURITY DESIGN STANDARDS

1. **PURPOSE.** This appendix establishes the Facility Security Management Program (FSMP) design standards for child care centers (CCC).

2. **LOCATION.**

a. CCC's shall, wherever possible, not be collocated within the perimeter of FAA facilities.

b. When this is not possible, additional protective measures shall be required to ensure that the CCC is designed and built to provide an increased level of risk reduction to explosive attack and other major criminal and terrorist threats.

3. **CHILD CARE CENTER DESIGN.**

a. The FSMP shall be an integral part of the planning and design for all CCC facilities for which the FAA exercises design and construction responsibilities.

b. The regional and center servicing security element (SSE), must evaluate all design, development, and engineering plans for CCC's, as well as leased facilities for FAA Child Care Centers.

4. - 10. **RESERVED.**

SECTION 1. BASELINE SECURITY DESIGN STANDARDS.

11. FACILITY PLANNING AND DESIGN.

a. Once a decision is made to select, construct, or reconfigure a facility or office space, or move to another facility or office space, security considerations for the CCC shall be an integral part of the planning, design, and construction process.

b. Program and project managers responsible for the design and development of CCC's to be located on or in close proximity to FAA facilities shall coordinate with the SSE to ensure that recommendations and requirements identified by the SSE are included in project and program funding.

c. All drawings, design specifications, and statements of work shall be available to the SSE for review and comment.

d. It is understood that site specific adaptations may be necessary to comply with local building and licensing codes.

e. Department of Transportation and FAA policy require that any agency sponsored CCC be locally licensed.

12. LOCKS.

a. The FAA standard locking "Best Lock" system, shall be installed on all exterior and interior doors requiring locking capabilities.

b. FAA shall ensure that all exterior doors have nonremovable hinge pins or exterior hinge pins that have been modified to prevent removal.

13. ENTRANCE DOORS.

a. FAA shall use solid core doors on the main entrance doors.

b. A closed circuit television (CCTV) video camera is required and shall be installed by the FAA when the center entrance is not visible to center staff.

c. An electronic key pad access system with key override and large buttons for ease of use for the disabled (for authorized entrance without staff monitoring) shall be installed by FAA.

14. OTHER DOORS.

a. Solid core doors shall be installed on all main corridor areas and building side doors that allow access to class rooms.

b. FAA shall install the agency Best Lock locks, on all exterior doors of the facility, as well as on all interior doors that need to be secured.

c. The FAA design architect in coordination with the SSE shall determine the specific "Best" locking device based on the area functions (administrative, privacy, storage, etc.).

d. Half window doors may be used only on interior doors if they provide the strength and/or the limited size necessary to prevent forced entry into classroom areas. Standard doors may be installed in all other common areas (bathrooms, supply areas, janitor closets, etc.).

15. PANIC DOOR HARDWARE.

a. Panic hardware (emergency situation use) shall be installed on all exit doors by FAA.

b. Emergency exit doors shall preclude entry from the outside and should be alarmed to detect entry attempts.

16. - 25. RESERVED.

SECTION 2. PHYSICAL SECURITY ASSESSMENT.

26. ASSESSMENT.

a. CCC structures located on or planned for location on FAA property with other FAA facilities shall have a comprehensive physical security assessment conducted prior to actual construction. Security engineering concepts shall be applied to facility design criteria.

b. The measures addressed in subsequent paragraphs of this section shall be applied in accordance with the results of the physical security assessment and security engineering of the facility design conducted by the SSE in conjunction with ANI design engineers. Consideration shall be given to installing a remote duress signal from the CCC to the ARTCC or the local police department.

27. STANDOFF (SETBACK) DISTANCE REQUIREMENTS. In the event it is determined that a CCC shall be collocated on a site with an ARTCC, the following standoff distances shall be mandatory:

a. Not less than 200 feet from ARTCC Building and other critical assets.

b. Not less than 200 feet from the main entrance(s) to the facility.

c. Not less than 100 feet from the perimeter fence in the final design location.

28. GLAZING. The design and installation of the protective window glazing measures covered in this section shall be accomplished under the direction of an Airway Facilities engineer.

a. Laminated and heat treated glass shall be used by FAA for new construction and security film for retrofitting CCC's.

b. When security film is used in a retrofit condition, care shall be taken in developing appropriate specifications. Not all film on the market is true security film which shall enhance survivability under blast loads. A minimum of 7 mm thick security film shall be used.

29. - 39. RESERVED.

SECTION 3. PLAYGROUND DESIGN.

40. PERIMETER BARRIER.

a. Playgrounds of CCC's collocated with FAA facilities shall be enclosed by fences at least 48-inches high within the perimeter fence of the facility.

b. The playground fence is separate and distinct from the overall CCC perimeter barrier. Playground fence construction shall:

(1) Be of a safe design with full caps and no filials or picket tops.

(2) Be designed to discourage climbing.

(3) Not have openings in the fabric that exceed 3.5-inches on any side.

(4) Have a gate that is self-closing and latching.

41. - 50. RESERVED.

SECTION 4. SECURITY PROTECTIVE MEASURES.

51. EQUIPMENT. Minimum baseline CCTV risk reduction measures shall be incorporated into the design and construction of each FAA CCC to include the following:

a. CCTV camera on exterior of main entrance door.

b. CCTV monitor in the CCC reception area.

c. Emergency electrical power backup supply capable of running the security equipment for 90 minutes in the event of a commercial power outage.

d. Video recording and monitoring capabilities.

e. Video tape storage and handling procedures.

52.– 60. RESERVED